2021-09

ASSESSING AND VISUALIZING RISK IN MONTEREY PHOENIX THROUGH A SUPPLY CHAIN CYBER-ATTACK USE CASE

Palmieri, Margaret

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ASSESSING AND VISUALIZING RISK IN MONTEREY PHOENIX THROUGH A SUPPLY CHAIN CYBER-ATTACK USE CASE

by

Margaret Palmieri

September 2021

Thesis Advisor:	Kristin M. Giammarco
Second Reader:	Bonnie W. Johnson

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2021	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE ASSESSING AND VISUALIZING RISK IN MONTEREY PHOENIX THROUGH A SUPPLY CHAIN CYBER-ATTACK USE CASE	**5. FUNDING NUMBERS**
6. AUTHOR(S) Margaret Palmieri	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

This thesis explores how decision makers could use the Monterey Phoenix (MP) behavior modeling tool developed at the Naval Postgraduate School to assess, visualize, and prioritize cyber risk in a supply chain. Assessing supply chain risk is a complex problem because of the inter-relationships among various parts of the system and between the system and its environment. This thesis applies and extends a reusable methodology to analyze risk in MP, developed by Navy LCDR Richard Moebius in 2018, to the use case of a cyber-attack on a jet fuel supply chain, first modeled by student interns from the National Security Agency. It assesses and displays risk for single- and multi-threat use cases, and for the first time, adds the global report to an MP model for assessing risk. It demonstrates how MP can overcome the limitations of existing tools, like the risk table, risk map, and risk matrix. For example, MP automatically generates an exhaustive list of potential risk scenarios; MP sequence diagrams provide context on the system, its environment, and relationships among different risks; MP easily and quickly updates the model to support "what if" questions; and MP displays aggregate and average risk across the system and sorts scenarios by a user-defined risk threshold. Finally, the work describes how decision makers from different backgrounds can interact with the MP model to improve their understanding and prioritization of risk.

14. SUBJECT TERMS risk, risk assessment, risk management, system, system of systems, complex system, Monterey Phoenix, MP, modeling, visualizing risk, cyber risk, cyber security, supply chain, Colonial Pipeline, hack, resource prioritization, global report, risk matrix, risk map, risk table, cyber-attack, cyber threat, Moebius, NSA, Giammarco, Auguston, Alden	**15. NUMBER OF PAGES** 103
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

ASSESSING AND VISUALIZING RISK IN MONTEREY PHOENIX THROUGH A SUPPLY CHAIN CYBER-ATTACK USE CASE

Margaret Palmieri
Civilian, Department of the Navy
BA, Rutgers University, 2004
M, Rutgers University, 2005

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2021

Approved by: Kristin M. Giammarco
Advisor

Bonnie W. Johnson
Second Reader

Oleg A. Yakimenko
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis explores how decision makers could use the Monterey Phoenix (MP) behavior modeling tool developed at the Naval Postgraduate School to assess, visualize, and prioritize cyber risk in a supply chain. Assessing supply chain risk is a complex problem because of the inter-relationships among various parts of the system and between the system and its environment. This thesis applies and extends a reusable methodology to analyze risk in MP, developed by Navy LCDR Richard Moebius in 2018, to the use case of a cyber-attack on a jet fuel supply chain, first modeled by student interns from the National Security Agency. It assesses and displays risk for single- and multi-threat use cases, and for the first time, adds the global report to an MP model for assessing risk. It demonstrates how MP can overcome the limitations of existing tools, like the risk table, risk map, and risk matrix. For example, MP automatically generates an exhaustive list of potential risk scenarios; MP sequence diagrams provide context on the system, its environment, and relationships among different risks; MP easily and quickly updates the model to support "what if" questions; and MP displays aggregate and average risk across the system and sorts scenarios by a user-defined risk threshold. Finally, the work describes how decision makers from different backgrounds can interact with the MP model to improve their understanding and prioritization of risk.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CRA	Cyber Risk Assessment
DFSP	Defense Fuel Supply Point
DLA	Defense Logistics Agency
DOD	Department of Defense
ERM	enterprise risk management
JBA	Joint Base Andrews
MP	Monterey Phoenix
MPVIP	Monterey Phoenix Virtual Internship Program
NAVAIR	Naval Aviation Systems Command
NCR	National Capital Region
NSA	National Security Agency
USAF	U.S. Air Force

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The May 2021 ransomware attack against the Colonial Pipeline, which transports fuel along the Eastern Seaboard of the U.S., highlighted the vulnerability of American infrastructure, specifically the fuel supply chain, to cyber-attack. It also prompted the president of the United States to issue Executive Order number 14028 to improve the ability of the federal government to identify, deter, safeguard, and respond to cyber threats.

This thesis explores how the Monterey Phoenix (MP) behavior modeling tool developed at the Naval Postgraduate School (NPS) could help decision makers assess, visualize, and prioritize cyber threats to a supply chain. The thesis demonstrates a repeatable and extendable methodology for assessing risk in MP, and how MP allows decision makers to have a common understanding of how the supply chain works end-to-end and at specific nodes through tailoring the model. It finds the benefit of using MP to assess risk increases as use cases grow in complexity, and MP provides the ability to visualize risk more comprehensively than existing risk assessment tools.

Systems engineers have traditionally used MP, a lightweight formal methods behavior modeling tool, to model software architectures and support verification, validation, and improvement of system designs. Two student research efforts (Moebius 2018; Alden et al. 2020) demonstrated the potential to apply MP beyond its software and systems engineering roots, and they inspired the research question of this thesis: how could decision makers use MP to assess, visualize, and prioritize cyber risk in a supply chain?

To answer the research question, the thesis methodology builds upon the students' prior research. It applies and extends a methodology for using MP to assess system risk developed by Navy Lieutenant Commander Richard Moebius in his master's thesis (2018). The Moebius methodology has seven steps: create a behavioral model of the intended operation; add negative alternatives to the operation; add risk attributes (e.g., impact and likelihood); calculate or assign impact to negative outcomes; calculate or

assign likelihood to negative outcomes; use impact and likelihood to calculate risk; and output desired format of risk for decision makers (Moebius 2018, 16–17). This thesis applies the Moebius methodology to the use case of a cyber-attack on a military jet fuel supply chain, first modeled in MP by a group of student interns from the National Security Agency's Monterey Phoenix Virtual Internship Program (MPVIP) as part of their capstone project (Alden et al. 2020).

This thesis also extends the Moebius methodology by applying the global report function in MP to risk assessment for the first time. The global report function conducts queries across all event traces for information the modeler prescribes. Then, it displays the information in a concise report card at the top right of the model screen, and it marks the traces that contain the prescribed information. This thesis uses the global report to identify the total and average risk across all traces in the model, the highest risk and its corresponding trace, and which traces in the model meet a prescribed risk threshold. The modeler can then sort the traces by those marked using the standard sort menu in MP. As a result of adding the global report, this thesis extends Moebius' methodology and renames step six to account for the new actions of querying and sorting risk.

The thesis applies the extended Moebius methodology and demonstrates the utility of MP in supporting risk assessment through three models related to the use case: one to calculate the risk of a cyber-attack on the Colonial Pipeline, another to calculate the risk of a cyber-attack on barge operations that transport fuel in the supply chain, and a third to calculate the risk of two cyber threats to the supply chain. Risk calculations use the simple risk model, which assigns a single variable for probability and impact (Smith and Merritt 2002, 21). This thesis uses the term likelihood instead of probability to reflect the fact that all measures in the use cases are notional. The jet fuel supply chain risk assessments demonstrate the ability of MP to help decision makers understand risk in systems of varying complexity. The barge use case demonstrates how MP can produce a smaller model to simplify or more deeply examine risk assessment in one specific aspect of the supply chain. The model of the Colonial Pipeline cyber-attack and the model with two cyber threats demonstrate the ability of MP to assess and visualize how negative alternatives impact the operation of the entire supply chain.

There are four main conclusions of this research.

1. The Moebius methodology is repeatable and extendable. There is enough rigor in the methodology to guide a modeler through using MP to assess risk, and enough flexibility for the modeler to tailor the model variables, risk calculations, and display output to the needs of different use cases and decision makers.

2. MP allows decision makers to achieve and assess a common understanding of how the supply chain works end-to-end and how cyber threats could impact different aspects of the supply chain. Tailoring the model can help decision makers resolve differences in knowledge, assumptions, and perspectives, which is especially helpful in addressing supply chain risk because decision makers often come from different organizations and backgrounds representing different aspects of the supply chain.

3. The benefit of using MP to assess risk increases as use cases grow in complexity. The global report for the simple barge model provided insight into the total and average risk across all the traces, but with only 3 total traces, it was not time consuming to manually review each trace. In the model with two cyber threats, MP returned 12 traces, making the global report and the marked traces much faster to digest than manual reviewing traces to find those of greatest interest. Additionally, the ability of MP to automatically generate 12 potential scenarios from the two-threat model was much faster—and potentially more effective—than having humans brainstorm and model those scenarios in a systems modeling language or other visualization tool. Reducing manual work developing and interpreting the model provides decision makers more time to discuss and debate risk mitigation strategies.

4. Finally, MP provides the ability to visualize risk more comprehensively than existing risk assessment tools. The risk table, risk map, and risk

matrix have limitations in how they communicate the context of the system, identify interdependencies among risks, respond to real-time "what if" drills, and display aggregate risk. MP has features that can overcome these limitations. For example, the sequence diagram in MP helps decision makers visualize the flow of events within and among the supply chain nodes, and it communicates important context about the system and its environment, including order and precedence, cause and effect, people and places, behavior attributes like timing, and interdependencies among risks. Understanding interdependencies can help decision makers develop different mitigation strategies, perhaps prioritizing contributing factors to address the root cause of a vulnerability over addressing more visible symptoms of an attack. Modelers can also easily update the assumptions and variables in the model and quickly rerun the simulation in seconds to regenerate scenarios and risk assessments so decision makers do not need to delay a decision waiting for updated analyses. Finally, MP visualizes aggregate risk through the global report, which displays total risk and average risk. This view allows decision makers to compare risk across multiple models and use cases.

Modeling risk in MP, especially supply chain risk, is still nascent research. Future research should improve upon the quality and type of assessments MP can do, the visualizations it creates to support decision makers, and the ability of the modeling software to handle more complex use cases. In the meantime, this thesis has unlimited distribution with the intent of sharing the Moebius methodology, and the extensions from this thesis, with analysts and decision makers so they can see the potential benefits of MP models in risk assessment.

References

Alden, Nathan, Jessica Dahl, Oybek Kamalov, Troy Smith, Rachel Talkington, Rachel Thompson, Noah Wells, and David Zhao. 2020. "Enterprise Risk Management." Unpublished presentation, July 25, 2020. https://nps.app.box.com/s/ber4qe65vzbk2lpip4nwvqm9euqxk5u1.

Moebius, Richard C. 2018. “Methods and Tool for Risk Analysis Based on Behavior Models Utilizing Monterey Phoenix.” Master’s thesis, Naval Postgraduate School.

Smith, Preston G. and Guy M. Merritt. 2002. Proactive Risk Management: Controlling Uncertainty in Product Development. New York, NY: Productivity Press.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This thesis would not exist without the guidance, expertise, and mentorship of Dr. Kristin Giammarco, associate professor in the Department of Systems Engineering at the Naval Postgraduate School (NPS). Her expertise in systems engineering and Monterey Phoenix (MP) guided the direction of this research and she actively contributed to this thesis by creating the functional code for the global report with help from Dr. Mikhail Auguston, Professor Emeritus in the Computer Sciences Department. I am especially grateful for her patience and encouragement while I completed this thesis and managed full-time employment and child care.

The team of National Security Agency interns who first modeled the military jet fuel supply chain were the inspiration for this thesis. I am exceptionally thankful for the contributions of Nathan Alden, a student intern from the University of North Georgia, who developed the MP code for the initial jet fuel supply chain risk model and provided key insight and guidance on modeling cyber risk in MP. I am also thankful for the work Richard Moebius put into his thesis to demonstrate how MP can model risk. I greatly appreciate the feedback of Dr. Bonnie Johnson, senior lecturer in the in the Department of Systems Engineering at NPS, as the second reader of this thesis.

The ability to pursue learning is a luxury I could only experience through the support of family, friends, and colleagues. Katie Houston, Julia Elman, and Cathy Watson cared for my daughter while I read, modeled, and typed. Cody Reese, Brad Garber, and Dr. Adi Zolotov provided exceptional encouragement and role models for lifelong learning. My supervisors at the Office of the Chief of Naval Operations, especially Admiral William Lescher and Admiral James Kilby, allowed me to take time to learn while I also led significant efforts for the Navy. The Digital Warfare Office team and systems architects across the Navy provided practical insights that motivated me to learn more about the engineering field so I could help them, and the Navy, solve tough problems. Finally, I am so thankful for the love and support of my husband, who never doubted why a public policy major would want to get an engineering degree, and my daughter, who I hope will someday be proud that I completed what I started.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

In early May 2021, DarkSide hackers affiliated with a Russia-linked cybercrime group conducted a ransomware attack against the Colonial Pipeline, which transports about 2.5 million barrels of fuel per day from the Gulf Coast of the United States to its Eastern Seaboard as part of the U.S. fuel supply chain. The attack resulted in the Colonial Pipeline Company closing the pipeline for five days, causing gas shortages, long lines at the pump, and higher fuel prices across the Eastern U.S. The Colonial Pipeline Company also paid DarkSide $4.4 million in ransom to prevent them from leaking about 100 gigabytes of data they stole in the attack (Turton and Mehrotra 2021). The cyber-attack highlighted the vulnerability of American infrastructure, specifically the fuel supply chain, to cyber-attack, and prompted the President of the U.S. to issue Executive Order number 14028 to improve the ability of the federal government to identify, deter, safeguard, and respond to cyber threats (Sigalos 2021). This thesis explores how the Monterey Phoenix modeling tool developed at the Naval Postgraduate School (NPS) could help decision makers assess, visualize, and prioritize cyber vulnerabilities in a supply chain and inform mitigation options to improve the resiliency of the chain. This chapter discusses the motivation for the thesis, the thesis research question, the scope of the thesis, and the benefits of this study. It also provides an overview of the organization of the thesis.

A. MOTIVATION

Recognizing vulnerability, understanding risk, and prioritizing mitigation measures in a supply chain is a complex problem because of the inter-relationships of various parts of the system. It would be beneficial for humans to have tools to help them estimate, visualize, and prioritize cyber risk. One candidate tool is Monterey Phoenix (MP), a lightweight formal methods behavior modeling tool designed by faculty and students at NPS. Systems engineers have used MP to model software architectures and support verification, validation, and improvement of system designs by modeling and experimenting with potential system behaviors early in the life cycle.

In the summer of 2020, a group of student interns from the National Security Agency (NSA) used MP in a new way: to model a cyber-attack on a jet fuel supply chain (Alden et al. 2020). The interns' work demonstrated the potential for MP to expand beyond its software and systems engineering roots. After seeing the interns' presentation, this author wondered if MP could be a useful tool for helping decision makers assess, visualize, and prioritize risks across a system to best allocate limited resources for risk mitigation. Personal experience provided numerous anecdotes of executives struggling to understand and act on system-wide cyber risk, especially when different organizations owned or operated different parts of the end-to-end system. Challenges in decision making often resulted from:

- Siloed views regarding system vulnerabilities, which could bias executives to prioritize the part of the system they knew most, or scapegoat the part of the system they knew least
- Lack of a common framework through which executives could share and compare their assessments of vulnerabilities and mitigations that also provided transparency into the thinking and data underpinning those assessments
- Lack of a common visualization tool that showed the end-to-end system context to allow more in-depth conversations about how various vulnerabilities and mitigations impact the whole system and not just a single node
- The need to reschedule decision meetings because those in the room could not answer "what if" questions related to changes in assumptions, risk tolerance levels, or other updated factors because experts needed time to recalculate their assessment based on new information

The interns' presentation highlighted several features in MP that could potentially address these challenges, including the ability to:

- Model systems, processes, capabilities, organizations, actors, and environments to account for and display the various elements of a system end-to-end
- Identify the behaviors and interactions that occur among the elements to understand dependencies, gaps, and seams that might exist in the system or among organizations that manage and operate the system
- Quantitatively calculate and visually depict both single node and system-wide behavior to understand how a node fits into the broader system context
- Visually present information so even non-technical observers can interpret the model, making complex systems easier to understand and analysis more board-room-ready
- Provide instantaneous feedback on changes to the model, which could support "what if" questions more readily and, ideally, lead to more timely decisions

This thesis explores these features to understand how MP might be a useful tool for supporting decision makers in assessing and visualizing risk. It builds on the NSA interns' thoughtful work, and an earlier work by Navy LCDR Richard Moebius (2018) that demonstrated a reusable methodology in MP to analyze risk. By applying and extending the Moebius methodology to the interns' jet fuel supply chain cyber-attack use case, this thesis demonstrates the extent to which decision makers could leverage MP to assess, visualize, and prioritize risk across a system. This kind of tool could be particularly helpful to executives as they determine how to allocate limited resources to mitigate cyber risks.

The research on the use case in this thesis started about a year before the real-world cyber-attack on the Colonial Pipeline, yet the jet fuel supply chain use case features a similar attack. The parallel to real-world events, and the spike in the national dialogue about vulnerabilities in U.S. critical infrastructure as a result of the cyber-attack

on the Pipeline, suggest there is a need for better tools to help decision makers assess and prioritize supply chain risk. The events also invigorated the motivation behind this thesis.

B. RESEARCH QUESTION

How could decision makers use the Monterey Phoenix (MP) behavior modeling tool to assess, visualize, and prioritize cyber risk in a supply chain?

C. SCOPE OF THESIS

The scope of this thesis is to apply and extend a reusable methodology developed by Moebius (2018) for modeling risk in MP and demonstrate its application on the use case of a cyber-attack on a military jet fuel supply chain. The extension of the Moebius method includes the introduction of the global report function in MP to calculate and summarize risk across a series of events. The thesis assumes knowledge about the use case that is publicly accessible online. It cannot answer questions pertaining to behavior or risk outcomes in the jet fuel pipeline that may be classified or that have not been documented publicly. This thesis does not describe how to model in MP since that methodology has been documented in other research publications as well as in MP handbooks and tutorials (Auguston 2009 and 2020; Giammarco and Auguston 2019; Monterey Phoenix Home n.d.).

D. BENEFITS OF STUDY

This thesis demonstrates how MP models may be used to better assess and prioritize risk in a supply chain. Even though executives must frequently make decisions about how to allocate limited resources to mitigate risk in systems, they do not fully leverage the capabilities and visualization available in MP today. This thesis helps executives, systems engineers, and cyber security experts become more informed of the potential for MP to support risk assessment and prioritization decisions, and it recommends ways to enhance MP capabilities to support risk assessment in the future.

This thesis also makes the Moebius methodology accessible to a broader audience. Moebius' thesis used government-sensitive examples to demonstrate his methodology, so his thesis distribution extended to DOD and DOD contractors only. This

thesis uses an unclassified example with unlimited distribution so non-DOD researchers—and practitioners—can learn from Moebius' pathfinding methodology and the extended methodology demonstrated in this thesis.

E. OVERVIEW OF THESIS

The next chapter of this thesis provides an overview of related works, including a literature review, discussion of current risk assessment tools, and description of the two student works underpinning this research. Chapter III describes the methodology this thesis uses. Chapter IV applies the methodology to the jet fuel supply chain use case and extends the Moebius methodology by adding the global report. Chapter V presents conclusions and recommendations for further research. The Appendix contains the MP code for the models discussed in the thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

II. RELATED WORKS

This chapter reviews existing work related to this thesis. It presents a summary of related literature, a comparison of the features of current risk assessment approaches and those of MP, and an overview of the two student projects this thesis directly builds upon.

A. LITERATURE REVIEW

There is an abundance of literature in risk management that includes textbook-style publications with broad and deep explanations on how to define, measure, and mitigate risk (Wolke 2017), as well as shorter executive publications from consultant firms like Booz Allen Hamilton, McKinsey & Company, KMPG, Boston Consulting Group, Price Waterhouse Cooper, and dozens of others, that provide advice on how to apply risk management to common business problems (Consultantcy.org 2018). There is literature that describes risk management in the context of project management (Project Management Institute [PMI] 2013) and product development (Smith and Merritt 2002), which address risk management planning, identification, analysis, response planning, and controlling risk to reduce the occurrence and impact of negative events in the project. Federal government agencies have developed organization-specific policies and methodologies for managing risk (National Aeronautic Space Agency [NASA] 2011; Office of the Deputy Assistant Secretary of Defense for Systems Engineering [DASD SE] 2017; Burke and Morgan 2018). These approaches use a variety of tools and techniques to assess risk. The next section discusses some of these approaches and compares them with features in MP.

There is also literature focused specifically on supply chain risk management (SCRM). A supply chain is a network of companies at different locations, also called nodes, which work together through links, or networks, to provide goods or services for end users (Goldsby et al. 2014, 6–7). SCRM literature defines and categorizes the variety of risks related to supply chain effectiveness and discusses strategies to manage and mitigate risk (Ho et al. 2015). There is also literature on enterprise risk management (ERM), which is an integrated and systemic approach to managing all the risks a

company faces (Dickinson 2001). Literature on the risk of cyber-attack in supply chains finds that supply chains require a holistic approach to risk management, and there is a need for empirical models and collaborative approaches to increase supply chain cyber resilience (Ghadge 2019).

Finally, there are multiple publications on MP that describe how the modeling tool works and ways to use it to design, validate, and verify system and system-of-system architectures and behaviors. These works highlight the objective of MP to provide a framework for specifying system behaviors, its parts, and its environment, as well as interactions among them. Most works also the benefits of MP, including its ability to identify unintended behaviors, to highlight constraints on behavior and dependencies among actions involved in the behavior, and to provide different ways to visualize behaviors (Auguston 2020, 6). This thesis also leverages MP tutorials for best practices on how to use MP (Giammarco and Auguston 2019).

B. CURRENT RISK ASSESSMENT APPROACHES

A key motivation for this thesis was exploring how MP could help decision makers improve their ability to prioritize risk compared to existing approaches. Prioritization decisions depend heavily on the quality of the risk assessment, as well as on the ability to communicate that assessment effectively to decision makers. This section discusses two limitations of current risk assessment approaches and the unique features of MP that could help overcome those limits.

1. Blind Spot Limitations

First, current risk assessment approaches rely heavily on humans to think of all possible negative consequences when assessing a system (NASA 2017, 43; Burke and Morgan 2018, 6–7). NASA has one of the most comprehensive guides to risk management available. At more than 230 pages, it outlines multiple rigorous techniques, tools, and heuristics for risk informed decision making, including evaluating the risk analysis for bias and verifying and validating the analysis with engineering tools and methods (NASA 2011, 65). The Cyber Risk Assessment (CRA) process used by Naval Aviation Systems Command (NAVAIR) also uses a systematic, analysis-rich approach to

assessing risk (Burke and Morgan 2018, 6–7). Yet, NASA and NAVAIR rely primarily on stakeholder input and system decomposition models as the main way to identify system vulnerabilities and alternatives (NASA 2011, 43; Burke and Morgan 2018, 5). Even the quality checks NASA conducts occur only on previously identified risks and alternatives. In other words, if someone does not think about a specific scenario occurring, it will not appear in the risk assessment. Former Secretary of Defense Donald Rumsfeld famously called these risks "unknown unknowns" (Rumsfeld 2002). These blind spots could result in suboptimal risk mitigation approaches, wasted resources, or worse outcomes if unidentified risks occur and the organization is unprepared to address them.

MP helps overcome human limitations by automatically generating scenarios that could result in risk. MP models the behavior of each component of the system separately from the behaviors that result from systems interacting with each other and their environment. Rather than relying on humans to manually specify the scenarios they can conceptualize, MP automatically generates all possible expressions of system behavior, within the model scope,[1] that could result from the system design, even scenarios that humans may not anticipate or that they may rule out as a result of biases (Giammarco et al. 2014, 205–208). MP exposes human blind spots so decision makers can be confident they are considering all possible risks, not just those humans were able—or willing—to identify.

The scope-complete scenario coverage feature of MP is especially beneficial as systems, and systems-of-systems, grow in complexity. Complex systems have more possible configurations and behaviors, including emergent behaviors, than humans can comprehend on their own (Giammarco et al. 2014, 204). Additionally, complex systems often touch numerous stakeholders, including designers, owners, operators, maintainers, resource allocators, information managers, and more, making coordination of all

[1] Scope is a limit the modeler sets on how many iterations MP will conduct on events in the model that occur multiple times (Quartuccio and Giammarco 2019, 394-395). For example, computer programs often include loops to repeat a specified action multiple times until a certain outcome occurs (Kodable 2019). MP would run that loop the number of times set by the scope in the model.

stakeholder viewpoints on the model time intensive. Organizations can make better use of stakeholder time by asking them to provide feedback on the exhaustive set of MP-generated scenarios, instead of relying solely on brainstorming sessions trying to come up with potential options.

2. Visualization Limitations

The second common limitation of existing risk approaches is in how they present risk assessment results. Regardless of whether analysts use simple or sophisticated analysis tools to calculate risk, they usually present the results of the analysis to decision makers in the form of a risk table, risk map, or risk matrix (Smith and Merritt 2002; NASA 2011; PMI 2013; DASD SE 2017; Burke and Morgan 2018). These three formats are simple and familiar visualizations, but alone they limit the type and depth of information presented on the risk assessment in a decision forum. NASA's risk management guide highlights the importance of tailoring the presentation of risk analysis to the needs of decision makers, and including a variety of results, including scenario descriptions, risk results, and sensitivity studies, to ensure decision makers have the information they need to make informed decisions about risk management (NASA 2011, 64). This section provides an overview of the risk table, risk map, and risk cube formats, their limitations, and the features in MP that could improve the visualization of risk beyond what these formats alone provide.

a. Risk Table

A risk table conveys information through the rows and columns of a spreadsheet. Tables can present a variety of information from a risk assessment, including the relationship among risk attributes (Smith and Merritt 2002, 158), risk attribute values (Smith and Merritt 2002, 78), risk priorities and urgency (NASA 2011, 138; Smith and Merritt 2002, 88), a description of risk consequences (NASA 2011, 109), and any other information that fits neatly in rows and columns. Figure 1 shows an example of a risk table from the NASA risk handbook (NASA 2011, 87). It describes four alternatives a decision maker could choose and the risk each option has in meeting four different criteria—time to completion, project cost, data volume, and planetary contamination—as

well as total risk for each option. It includes color coding to draw the viewer's eye to different levels of risk more quickly. Well-constructed tables, like this one, provide information-rich visualizations in a clear and concise way for decision makers.

Planetary Science Mission Imposed Constraint Risk Matrix

Alternative		Imposed Constraint Risk			
	Time to Completion	Project Cost	Data Volume	Planetary Contamination	Total*
	Constraint (< 55 months)	Constraint (<$500M)	Constraint (> 6 months)	Constraint (< 0.1% prob.)	
1. Propulsive Insertion, Low-Fidelity Science Package	2.8%	22%	4.1%	1.1%	25%
2. Propulsive Insertion, High-Fidelity Science Package	2.4%	57%	6.4%	3.2%	62%
3. Aerocapture, Low-Fidelity Science Package	3.0%	9.7%	8.7%	5.5%	18%
4. Aerocapture, High-Fidelity Science Package	2.3%	47%	12%	12%	57%

Figure 1. NASA Imposed Constraint Risk Matrix. Source: NASA (2011).

Despite their approachability, there are three key limitations of a table.

- **Context**: Risks appear out of context when presented in a table, so decision makers need to be familiar with the design of the system, including the function and behavior of system elements, the relationships among different elements of the system, and the relationships the system has with its environment in order to fully understand the risk information presented in the table.

- **Interdependencies**: A table cannot convey the interdependencies among risks, since each row and column represent individual scenarios or risks (NASA 2011, 143). Knowing possible dependencies among risks could help decision makers identify strategies that mitigate aspects of multiple risks at once, instead of a single risk at a time. Without the knowledge of these connections, that approach to mitigation is not available for decision makers to consider.

- **Static Data**: Tables present a snapshot of the data from the risk assessment, meaning the data is disconnected from the models and analysis from which it came. This means analysts are unlikely to be able to answer "what if" questions from decision makers in the board room. They must take the questions for action, change the assumptions or risk attributes in their models or analytic tools, update the table, and reschedule the meeting with decision makers before mitigating the risks in question. This could unnecessarily waste time, especially if decision makers are not familiar with the system or the risks.

b. Risk Map

A risk map, like the example in Figure 2, plots each risk on a graph with an x-axis representing impact and y-axis representing likelihood. The graph may also include one or more threshold lines to partition the graph into different sections that represent different risk tolerance levels (Smith and Merritt 2002, 35).

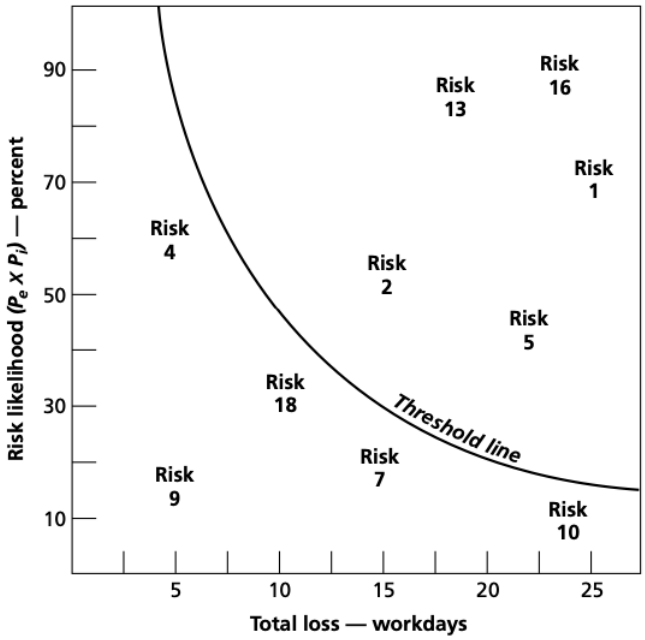

Figure 2. Risk Map. Source: Smith and Merritt (2002).

The benefit of a risk map is its ability to display both the likelihood and the impact of each single risk in comparison to all other potential risks. The visual display of how likelihood and impact contribute to overall risk helps decision makers simply and quickly see how many risks fall into each tolerance level, and why, so they can prioritize actions based on the attributes they value most (Smith and Merritt 2004, 212).

A risk map has the same limitations as a risk table: the risks appear out of context, meaning decision makers need to have some baseline level of familiarity with the system they are evaluating; risks on the map appear as individual, separate entities, which prevents decision makers from understanding interdependencies that could offer alternative mitigation options; and a risk map is a snapshot of data from the risk assessment meaning questions from decision makers may take more time to address if analysts need to rerun calculations back in their office.

A risk map has one additional limitation, as well: it cannot deal with aggregate risks (NASA 2011, 143). A risk map displays the total number of risks and how they spread above and below the threshold line, but it does not contain a value for total risk. If decision makers needed to compare the risks of two or more different use cases, it would be hard to discern total risk by just comparing the risk maps for the different use cases, especially if there are many use cases to review.

c. Risk Matrix

The risk matrix is a popular way to display risk, especially within DOD (DASD SE 2017, 27–30; NASA 2011, 143–145). Similar to a risk map, the x-axis presents values for likelihood and the y-axis presents values for impact. The intersection of a likelihood and impact value creates a box, which is red, yellow, or green depending on where the box appears in the chart: red represents high risk in the upper right corner of the box, green represents low risk in the lower left corner of the box, and yellow represents medium risk in the diagonal strip in between the red and green corners (DASD SE 2017, 27). Figure 3 shows an example of a risk matrix from NAVAIR, which they use in their CRA method (Burke and Morgan 2018, 8). The figure demonstrates how an organization can customize the attributes and values that underpin likelihood and impact based on the

type of risk being assessed. Like a risk map, it is quick and easy to see where risks fall at each tolerance level, allowing decision makers to prioritize the highest risk actions.

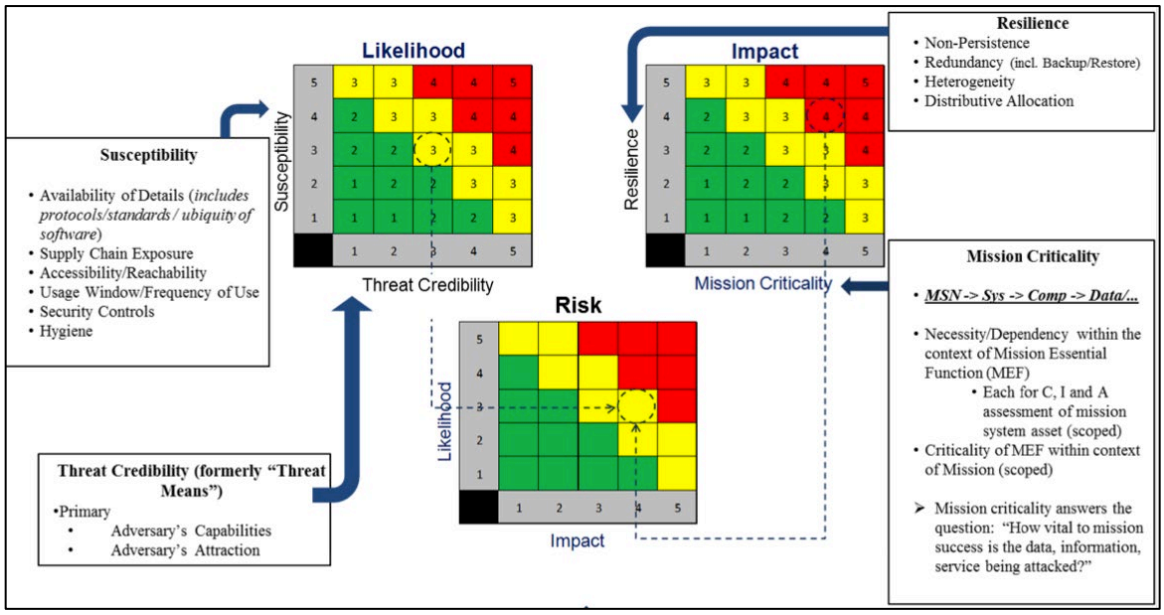

Figure 3. NAVAIR CRA Scoring Risk Matrix. Source: Burke and Morgan (2018).

The limitations of risk matrices echo those of risk tables and risk maps: risks appear out of context, they cannot convey interdependencies among risks, they present a snapshot of data, and they cannot visualize aggregate risks well. NASA uses a criticality ranking to prioritize risks then maps those rankings to the matrix, which helps overcome some aspects of the context and interaction limitations; however, it is unclear how widespread the use of such rankings is in DOD (NASA 2011, 144–145). Figure 3 shows NAVAIR uses mission criticality as one of the variables that underpin the impact score in their CRA method, but the method does not prioritize overall risk in the same way as NASA (Burke and Morgan 2018, 8). Additionally, the DOD risk guide directs program teams to base risk levels in the matrix on cost, schedule, and performance risk, then use additional factors, like time criticality and interrelationship of risks, to prioritize the risk after completing the matrix (DASD SE 2017, 27).

Even with factors included in the risk matrix to provide additional context and account for risk dependency, the risk matrix still presents a subset of data, and it cannot visualize aggregate risks well. Risk assessment would benefit from other tools that could provide context for risk in the system, convey interactions and dependencies among system elements and risk, present data in dynamic ways, and visualize aggregate risks.

d. MP Visualization Features

MP has several visualization features that could overcome the limitations of the risk table, risk map, and risk matrix. In MP's interactive environment, modelers separately define the behavior of the system from the interactions among systems and among systems and the environment, so the modeler has flexibility and control in describing how the system should behave (Quartuccio and Giammarco 2019, 395). MP automatically generates different use cases from the model and displays them in a sequence diagram with boxes for actors and events, and arrows for relationships (Auguston 2020, 7). The relationship arrows identify where interactions and dependencies exist between different parts of the model. These relationships can apply to systems and risks. Modelers can add tables and bar charts to the sequence diagram to display dependencies, as well. Modelers can also easily update the assumptions and variables in the model and quickly rerun the simulation in seconds to answer "what if" questions from decision makers in real time. The global calculation in MP can calculate values across use cases, which could display aggregate risks from the model. These features visually present information more comprehensively than a risk table, risk map, and risk matrix, and they inspired the research in this thesis on how MP can model and display risk in a supply chain.

C. MOEBIUS THESIS OVERVIEW

An earlier research effort that sought to demonstrate the ability of MP to model risk was a thesis completed by Navy Lieutenant Commander Richard Moebius in 2018. He recognized the potential of MP to evolve beyond its software and systems engineering roots to also support risk assessment. His master's thesis research question was, "Can a behavioral model implemented with Monterey Phoenix be used to analyze risk?" The

scope of the thesis was to demonstrate a reusable methodology to analyze risk and apply the methodology to four use cases (Moebius 2018, 2). The four examples Moebius used were the process fire order phase of a Mark 48 Advanced Capability torpedo launch sequence employed by U.S. submarines, a hydrazine bottle leak aboard a NASA spacecraft, an airline airport check-in kiosk process, and a Naval Air Systems Command (NAVAIR) cyber risk assessment (CRA) for a notional system (Moebius 2018, 30–55).

Moebius created a methodology, described in Chapter III, for using MP to model a system, calculate risk, and visually display the risk assessment results in the model. In subsequent chapters, this thesis applies and extends the Moebius methodology through a jet fuel supply chain use case and the addition of a global report.

D. NSA INTERN PROJECT ON ENTERPRISE RISK MANAGEMENT

The jet fuel supply chain use case in this thesis builds upon work done in 2020 by a team of NSA interns at NPS. As part of their summer capstone project, they used MP to model risk in two use cases: the effects of a cyber-attack on a jet fuel pipeline supply chain; and the impact former NSA contractor Edward Snowden had on the U.S. and Allied nations by leaking sensitive NSA information to the public (Alden et al. 2020). The MP models they created assessed operational impact, identified emergent behaviors, and determined financial, reputational, and mission consequences associated with each use case (Alden et al. 2020). They described MP as a tool organizations could use to bridge the gap between expert cyber security analysts and executive decision makers as part of a broader ERM process (Alden et al. 2020). They explained how their findings could inform ERM policies related to how much risk to take or where to invest resources in mitigations (Alden et al. 2020).

The NSA interns' research demonstrated how MP could model multiple nodes in a supply chain, introduce a cyber-attack as a bad actor in the system, and calculate potential immediate or delayed impacts of the attack (Alden et al. 2020). This thesis leverages the jet fuel pipeline model created by the NSA interns and modifies it to be capable of assessing risk across the supply chain. Chapter IV describes the NSA interns' model in more detail.

III. METHODOLOGY

This thesis applies and extends the Moebius methodology (2018) for using MP to assess system risk. Section A of this chapter provides an overview of the Moebius methodology. Section B describes the simple risk model, which this thesis uses to calculate risk as part of Step 6 of the Moebius methodology. Section C describes the global report function in MP and how it extends Step 6 of the Mobius methodology to query across all traces, identify aggregate risk, and mark traces of interest. The next chapter applies the extended methodology to the use case of assessing the risk of a cyber-attack on a military jet fuel supply chain.

A. MOEBIUS METHODOLOGY OVERVIEW

The Moebius methodology includes the following seven steps.

Step 1: Create a behavioral model of the intended operation. Behavior is the set of events that happens in a system or in the environment as it interacts with the system. Each event has a beginning and an end and may have a duration. Events also include two relationships—precedence and inclusion—that establish order. Precedence describes the sequence of events in time: one event precedes another, they happen concurrently, or they both happen without an ordering relationship (Auguston 2009, 1032–1033). Inclusion establishes a hierarchy of routines and sub-routines for each event (Auguston 2009, 1032).

Moebius (2018) employs the personification of interacting systems to highlight how modelers can think of system components and the environment as actors in the behavior model. Actors are producers or consumers of actions that impact mission completion. They could include adversaries, allies, or other systems (Moebius 2018, 15). Personification of systems is a helpful technique when designing behavior models for cyber and supply chain risk because it helps modelers identify both the technical and human elements of the system and its environment.

Moebius recommends scoping the model to include all the behaviors of all actors required to accomplish the mission, plus events that could detract from mission

accomplishment because the intent of the model is to evaluate the risk of mission failure. The sets of events among actors over time result in an observable outcome, which enables the evaluation of risk (Moebius 2018, 16).

Step 2: Add negative alternatives to the operation. To identify negative alternatives to mission accomplishment, consider the behavior of different actors in the system and the behavior that occurs in the environment. For example, one could modify existing actions so they are not performed or introduce new actions that result in outcomes different than mission accomplishment. The model will only evaluate the risk associated with negative alternative behaviors added to the model (Moebius 2018, 16).

Step 3: Add risk attributes. Once the behavioral model is complete, add attributes for risk, including probability and impact (Moebius 2018, 17).

Step 4: Calculate or assign impact to negative outcomes. Subject matter experts should define the values for the attributes added in the previous step, document the reasoning behind their opinions, then add those values to the model (Moebius 2018, 17).

Step 5: Calculate or assign likelihood to negative outcomes. Similar to Step 4, subject matter experts define the values for the attributes added in the previous step, document the reasoning behind their opinions, and add those values to the model (Moebius 2018, 17).

Step 6: Use impact and likelihood to calculate risk. Moebius gives flexibility to the modeler to determine how to calculate risk based on impact and likelihood recognizing that decision makers may prefer different approaches to evaluation. For example, one could average, multiply, add, or just display the values that contribute to risk (Moebius 2018, 17). The next chapter describes the approach this thesis takes to calculating risk, but Moebius' methodology, and the MP program itself, allow a variety of approaches. In fact, this flexibility is what allows this thesis to extend Moebius' methodology to incorporate the global report in MP.

Step 7: Output desired format of risk for decision maker. Similar to Step 6, Moebius gives the modeler the flexibility to display risk in a way that is most useful to the decision maker (Moebius 2018, 17).

B. RISK CALCULATION METHODOLOGY

Step 6 of the Moebius methodology allows the modeler to determine how to calculate risk based on impact and probability of risk. Multiple models, at varying levels of detail, exist for calculating risk. This thesis uses the simple risk model, which uses probability and impact to measure risk in the most streamlined way of all the models. In the simple risk model, probability includes the possibility of the risk event happening and the possibility of the various impacts occurring. The simple risk model defines drivers as the factors that both influence the risk event and its potential impacts. Because the simple risk model has the fewest categories and steps, it can mask certain nuances, such as risk that occurs when the probability of an event is low, but the probability of its impact is high. A higher fidelity risk model, like the standard risk model that tracks the probability and drivers for events and impacts separately, can improve risk resolution planning (Smith and Merritt 2002, 21–22). Figure 4 depicts the standard risk model and the simple risk model for comparison.

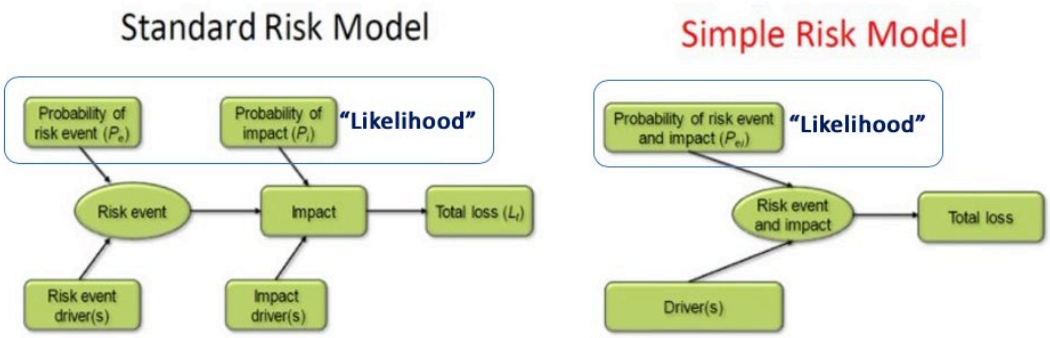

Figure 4. Standard and Simple Risk Model Overview. Adapted from Smith and Merritt (2017).

Figure 4 also notes that one can use probability or likelihood to understand the chance of an event or impact occurring. It is helpful to clarify the difference between probability and likelihood so decision makers understand how much confidence to have in the risk assessment. Probability conveys greater confidence because possible results are mutually exclusive and exhaustive, and they always sum to one. Likelihood conveys a

more hypothetical value and does not need to sum to one (Gallistel 2015). This thesis uses likelihood as the basis for risk analysis since all measures in the use cases are notional. To simplify readability, this document uses the term "likelihood" instead of probability from this point forward, recognizing that risk assessment can employ measures that vary in robustness, from notional to analytically-derived values.

C. GLOBAL REPORT OVERVIEW

Moebius demonstrated how MP can calculate risk for specific event traces. This thesis extends the Moebius methodology by adding the global report function in MP. The global report queries all event traces for information the modeler prescribes. Then, it displays that information in a concise report that appears as a small box in the top right of the model screen and it marks the traces containing the prescribed information.

To apply global risk, a modeler builds the global view in MP after first describing the intended behavior of the system and negative alternatives in the model. MP treats the global query, coded in the GLOBAL section of the MP schema, as an event itself, with $$TRACE being the code in the schema that reflects all event traces in the model. As an event, GLOBAL has its own attributes, which the modeler designates in the MP schema as GLOBAL.attribute_name. A modeler can establish values for the attributes using COORDINATE loops, which are interaction constraints in the MP schema, and different views of the model using SAY clauses, which tell MP what information to highlight on the screen. Once a set of traces exists, the global function accumulates calculations across the all the traces to identify the aggregate risk in the model, and it performs a global query across the traces to identify which traces have the characteristics the modeler prescribes (Auguston 2020, 107).

This thesis uses the global report to identify total risk, average risk, and those traces with the highest risk from a cyber-attack on the military jet fuel supply chain. The models in this thesis are simple, but they demonstrate the utility of the global report function, which only increases with more complex systems.

IV. APPLICATION OF METHODOLOGY

This chapter applies and extends the methodology developed by Moebius (2018) to the use case of a cyber-attack on a jet fuel supply chain. The sections progress through the seven steps of Moebius' methodology, each building out portions of the MP model for the use case. Step 6 extends the Moebius methodology by adding the global report in MP to query risk across all the traces and identify aggregate risks and traces of interest from the model. The chapter concludes with a discussion, in Step 7, of how to present the findings from the MP model to help decision makers understand and address risk associated with a cyber-attack on the jet fuel supply chain.

A. STEP 1: CREATE A BEHAVIORAL MODEL OF THE INTENDED OPERATION

The first step of the Moebius methodology is to create a behavioral model of the intended operation. Mobius recommends the model include all the events required to accomplish the mission, as well as events that could detract from mission accomplishment (Moebius 2018, 15–16). This section applies Step 1 of the methodology in three parts. First, it describes the behavior model for the intended operation of the end-to-end jet fuel supply chain. Then, it describes a simpler behavior model for the intended operation of the barge that moves jet fuel between two nodes in the supply chain to demonstrate how MP can tailored analysis to examine a subset of the supply chain. These two models are the foundation for applying the remaining steps of the Moebius methodology to the jet fuel supply chain use case. This section concludes by demonstrating an option in MP to incorporate additional attributes of the supply chain, such as the timing of events across nodes, to provide deeper insight into the behavior of the system.

1. Modeling the Supply Chain End-to-End

The intended operation of the jet fuel supply chain is transporting and refining a barrel of commercial Jet A fuel from the U.S. petroleum industry to Joint Base Andrews (JBA) where the military-grade F-24 fuel can be used for U.S. Air Force (USAF)

missions. The events required to accomplish the mission occur at five nodes in the supply chain (Inman 2017). According to the Defense Logistics Agency (DLA), which oversees the supply chains that ensure military aircraft have enough fuel to support mission requirements, these nodes and their corresponding events are:

1. **U.S. Petroleum Industry** – Produces commercial Jet A fuel and ships it to the Colonial Pipeline
2. **Colonial Pipeline** – Receives the Jet A fuel and transports the fuel to the Defense Fuel Support Point (DFSP) in Baltimore, Maryland
3. **DFSP Baltimore** – Receives Jet A fuel; transforms the Jet A fuel into F-24 military grade fuel by adding inhibitors for icing, static, and corrosion; puts the F-24 jet fuel in storage tanks; loads the F-24 fuel on a barge; and transports the fuel to the DFSP in Anacostia, Washington, D.C.
4. **DFSP Anacostia** – Receives the F-24 jet fuel, checks its quality and amount, and transports it via pipeline to tanks on JBA
5. **JBA** – Receives the jet fuel, and uses the fuel for USAF missions

Figure 5 displays the behavioral model for the intended operation of the jet supply chain. The Appendix Section A contains the code for the model.

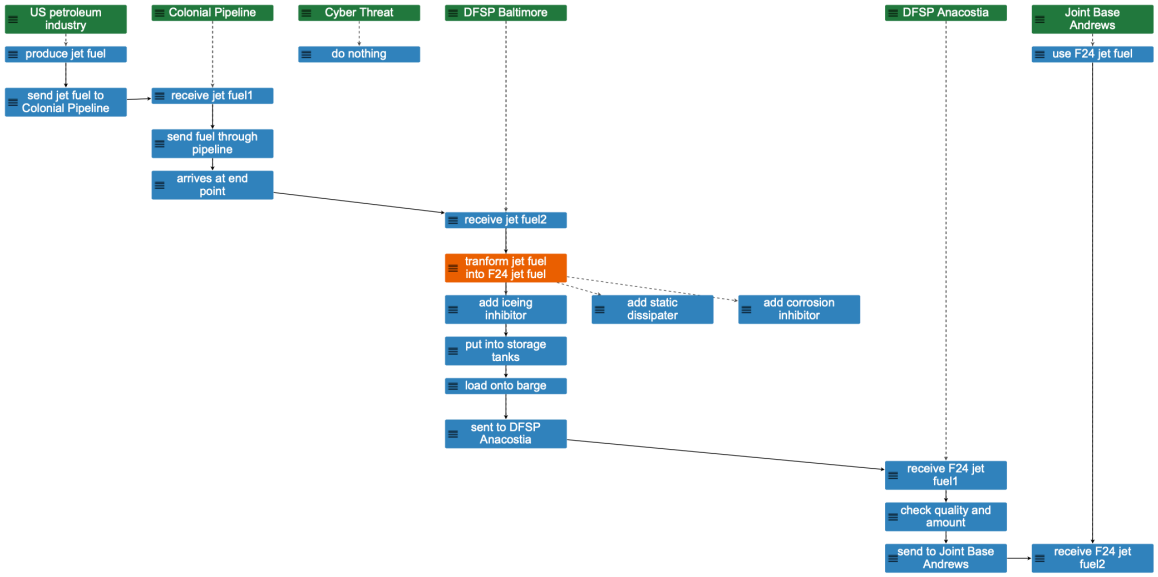

Figure 5. MP Model of the Intended Operation of the Jet Fuel Supply Chain (Scope 1, Trace 1). Source: Alden et al. (2020).

The model in Figure 5 accounts for all the major events described by Inman (2017) at each of the five nodes. It also includes a sixth node—a cyber threat—to account for events that could detract from mission accomplishment. The event associated with the cyber threat in the MP model in Figure 5 is "do nothing," which means the cyber threat has no impact on the jet fuel supply chain; the chain operates as intended. Step 2 of the Moebius methodology introduces negative alternatives to the intended operation of the system, which includes assigning cyber-attack events to the cyber threat. Step 1 of the methodology creates the baseline model to confirm the system works as intended before introducing any negative impacts.

2. Modeling Part of the Supply Chain

In addition to modeling the end-to-end supply chain to understand how a cyber-attack at one node impacts the system overall, one can model events in MP for just a subset of the supply chain. This more focused analysis may be useful when trying to simplify information for decision-makers, or when collecting or presenting more detailed evidence to support a specific finding or recommendation.

To demonstrate how MP can analyze a subset of the supply chain, the author partnered with Nathan Alden, one of the NSA student interns who developed the jet fuel supply chain model, to create a second, simpler model that expands on barge operations from the original jet fuel supply chain model. The barge model explores potential risk associated with a second possible cyber threat attacking the navigation systems on the barge that transports fuel from DSFP Baltimore to DFSP Anacostia. The barge is only a small part of the end-to-end supply chain model, but creating a tailored model for it in MP allows more in-depth analysis on its role and functions. The behavior model for the intended operation of the barge contains these two nodes with corresponding events:

1. **DFSP Baltimore** – Send barge to DFSP Anacostia
2. **Barge** – Leaves for DFSP Anacostia, arrives at DFSP Anacostia

Like in the end-to-end model, there is also a cyber threat in the barge model that could detract from mission accomplishment, but it has "no impact" in this step so the barge operates as intended. Figure 6 shows the tailored MP model for the intended operation of the barge. The Appendix Section B contains the code for this model.

Figure 6. MP Model of the Intended Operation of the Barge (Scope 1, Trace 3).

Step 2 of the Moebius methodology introduces negative alternatives to the intended operation of the barge. Figure 6 provides the baseline model to confirm the system works as intended before introducing any negative impacts.

3. Modeling Supply Chain Attributes

One of the benefits of MP is its ability to visualize both the flow of action within a node, and the relationships among nodes in the supply chain. This context allows the observer to understand various aspects of the supply chain in one view. The visual depiction of the MP model can communicate:

- Order and precedence (i.e., what comes first, next)
- Cause and effect (i.e., which actions cause which impacts)
- People and places (i.e., who is involved, where do things take place)
- Behavior attributes of the system (i.e., how long events take, how much events cost, how many people are required for each event, etc.)

The addition of behavior attributes in the model provides deeper insight into how the system works. For example, assume decision makers are interested in the impact of a cyber-attack on the amount of time it takes to send fuel from the U.S. petroleum industry to JBA because delays in fuel delivery could cause fuel shortages and impact jet availability for USAF missions. Per the Moebius methodology, Step 1 would establish the baseline for how long the supply chain takes to transport fuel to JBA when the system operates as intended. Modelers can create a timetable in MP and assign values to the duration of each event to calculate how long fuel spends at each node. Then, modelers can create a bar chart based on the timetable to visualize the timeline for fuel transportation through the supply chain. Figure 7 shows the MP display after adding the code for a timetable to the baseline model. The MP code is included in the model in the Appendix Section A. The timeline uses notional values for the duration of each event. Expert input could improve the accuracy of the timeline, or add additional attributes for cost or other specific impacts, but notional values for time are sufficient here to demonstrate the functionality MP has for modeling specific behavior attributes as part of the risk assessment.

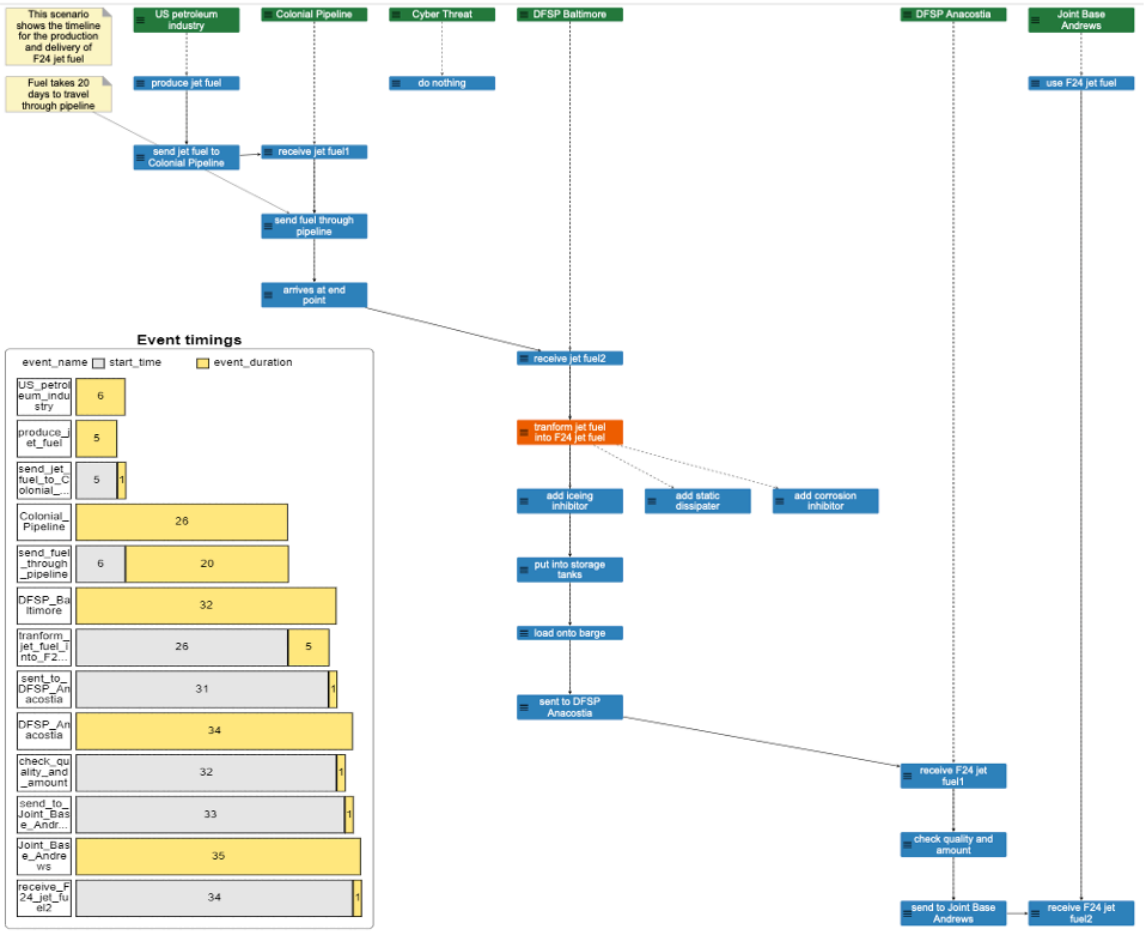

Figure 7. MP Model of the Intended Operation of the Jet Fuel Supply Chain with Timeline (Scope 1, Trace 1). Source: Alden et al. (2020).

The timeline bar chart provides more context on how the supply chain works, and it can identify interdependencies in the supply chain. For example, in Figure 7, the bar chart contains a yellow bar for each node in the supply chain that shows the total amount of time jet fuel spends at that node. There are also yellow and grey bars under each node that correspond to the events at that node. The yellow in the event bars depicts the length of time the specific event takes. The grey in the bars depicts the total time that node must wait for other nodes to complete their actions before starting its own operations. The last two bars in the chart depict the total time it takes for jet fuel to flow through the supply chain. If the supply chain operates as intended, it takes 35 days to send Jet A fuel from

the U.S. petroleum industry, convert it to F-24 military grade fuel, and send it to JBA. This baseline, and any deviation from it as a result of a cyber-attack, provide insight into specific behavior attributes of the system that may be of interest to decision makers. In addition to timelines, decision makers might want to explore the cost of each event or how many people are required for each event. MP has the flexibility to incorporate a variety of behavior attributes to improve understanding of system operations and different elements of risk.

B. STEP 2: ADD NEGATIVE ALTERNATIVES TO THE OPERATION

After establishing the model for the intended operation of the supply chain, the next step is to add negative alternatives; in other words, to add events that cause the supply chain to work not as intended. The two use cases in Step 1—the end-to-end jet fuel supply chain model and the barge model—included a cyber threat that had no impact on intended operations. This section assigns negative events to the cyber threat in each of the use cases in the form of a cyber-attack on the Colonial Pipeline and a cyber-attack on the barge navigation systems, respectively. It concludes with examples of other potential cyber threats that could impact the intended operation of the jet fuel supply chain.

1. Cyber-Attack on the Colonial Pipeline

In Step 2, the modeler adds the negative action of hacking the pressure control system of the Colonial Pipeline to the cyber threat in the jet fuel supply chain. They also add the potential impacts of the attack: the Pipeline bursts, the transportation of fuel halts until the Pipeline is repaired, and the Pipeline receives either light damage shown in Figure 8, medium damage shown in Figure 9, or heavy damage shown in Figure 10. The next step in the Moebius methodology assigns risk attributes to each event so decision makers can better understand the implications of each event on the end-to-end supply chain.

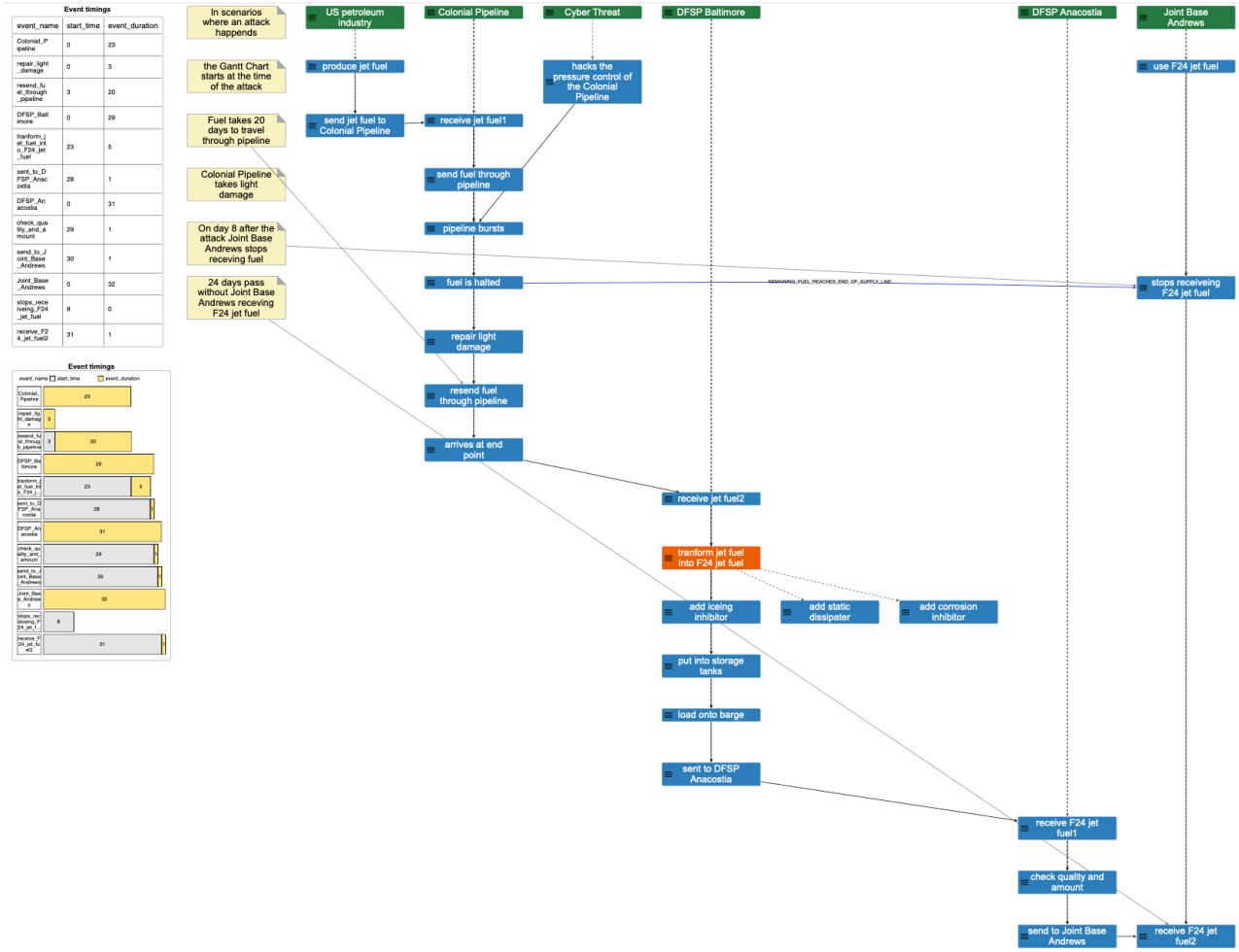

Figure 8. MP Model of Cyber Attack Creating Light Damage to the Colonial Pipeline (Scope 1, Trace 2). Source: Alden et al. (2020).

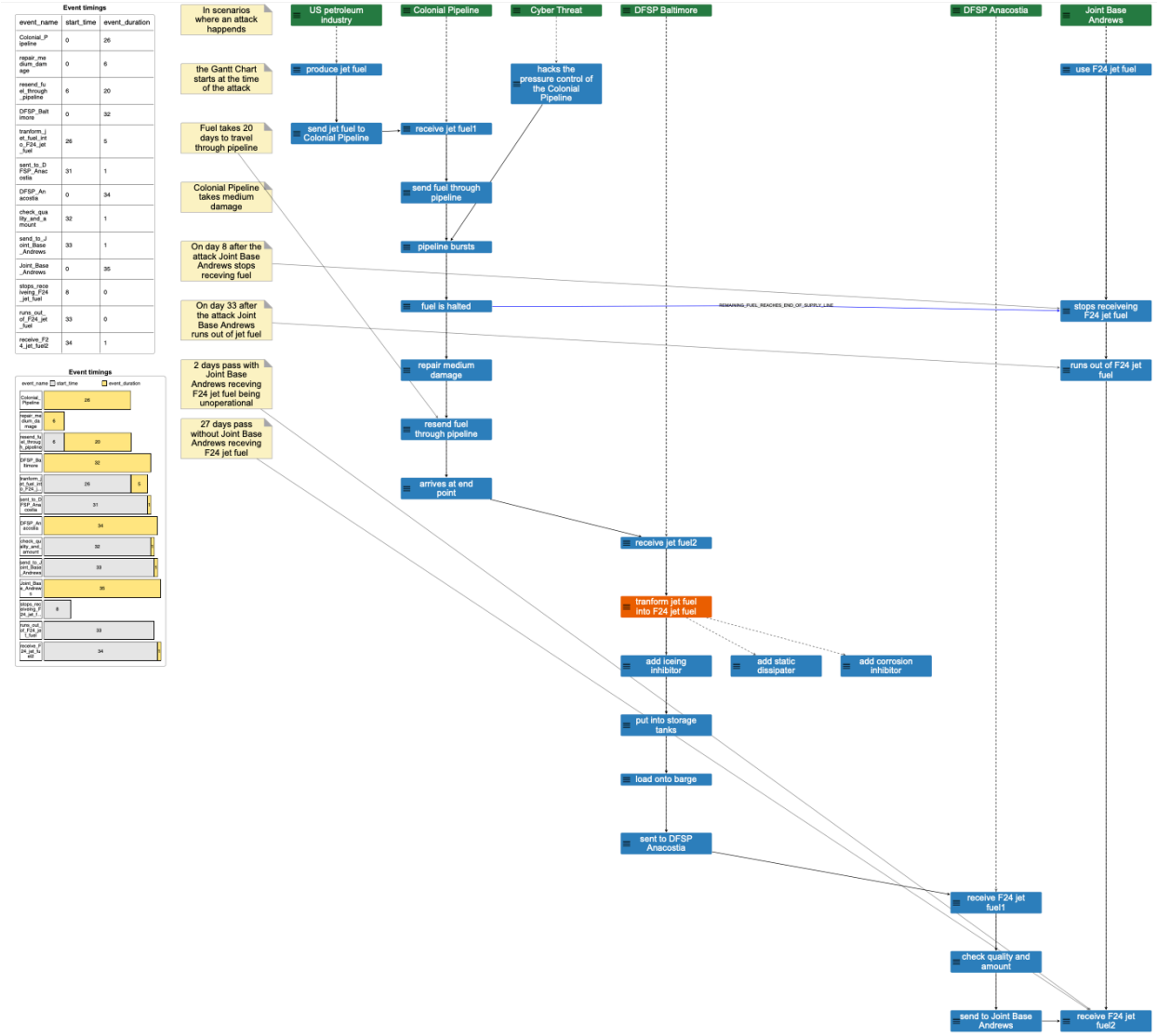

Figure 9. MP Model of Cyber Attack Creating Medium Damage to the Colonial Pipeline (Scope 1, Trace 3). Source: Alden et al. (2020).

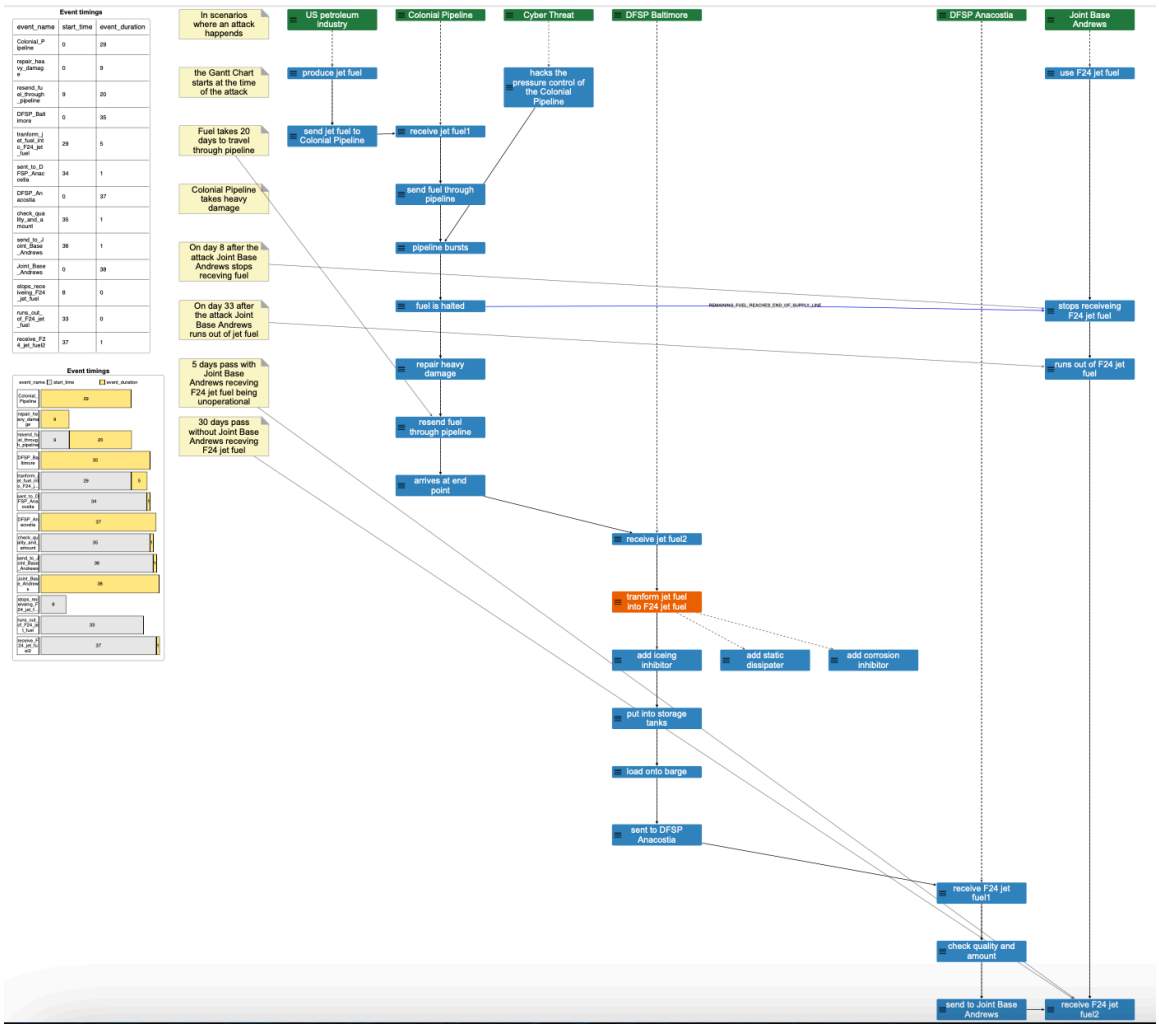

Figure 10. MP Model of Cyber Attack Creating Heavy Damage to the Colonial Pipeline (Scope 1, Trace 4). Source: Alden et al. (2020).

As with the model of the intended operations of the supply chain, the MP models with negative alternatives in Figures 8, 9, and 10 help visualize the flow of action within a node and the relationships among nodes in the supply chain. The models depict how a cyber-attack influences order and precedence, cause and effect, people and places, and with the bar charts included, timelines for the system's operations. The next chapter describes the results of this model in more detail.

2. Cyber-Attack on the Barge

In the model the author created to assess the risk of a second possible cyber threat attacking the navigation systems on the barge, two potential negative alternatives could occur: the attack either delays or sinks the barge. Figure 11 shows the scenario where the cyber-attack delays the barge. Figure 12 shows the scenario where the cyber-attack sinks the barge. The Appendix, Section B contains the MP code for this model.

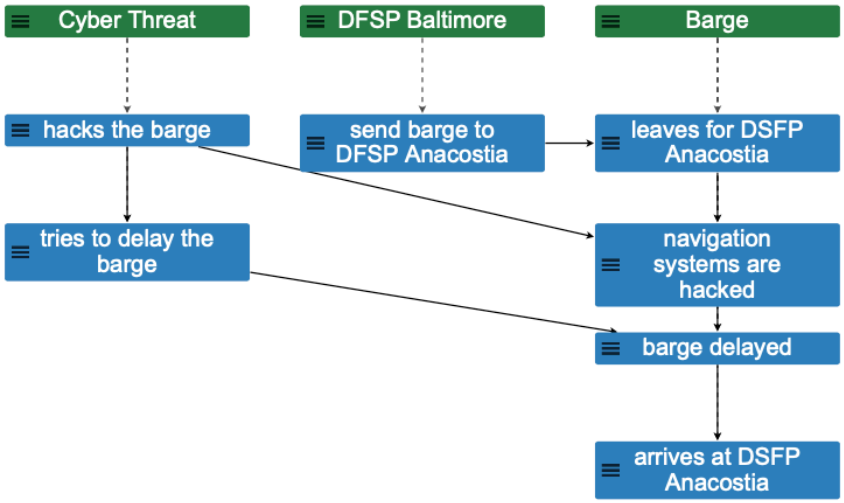

Figure 11. MP Model of a Cyber Attack Delaying the Barge (Scope 1, Trace 1).

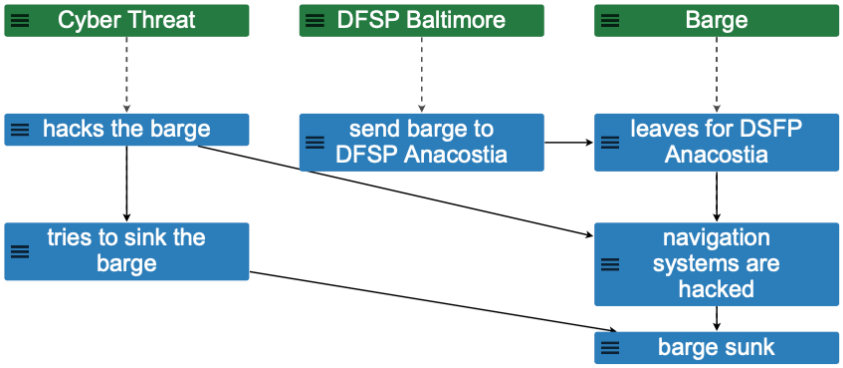

Figure 12. MP Model of a Cyber Attack Sinking the Barge (Scope 1, Trace 2).

The cyber-attack introduces new events in the model under the barge node: navigation systems are hacked, barge delayed, and barge sunk. The model helps visualize how the flow of action changes within and across nodes as a result of the attack.

3. Other Potential Cyber Threats

The MP model can facilitate brainstorming the various ways cyber threats could impact the supply chain because one can see the various nodes and events that are essential for mission accomplishment. Moebius recommends moving systematically through each actor and event in the system to identify the negative alternatives to include in the model (Moebius 2018, 16). Doing this for the jet fuel supply chain use case, one could brainstorm a variety of potential cyber vulnerabilities, such as

- An attack on the software that orders fuel, which could result in JBA receiving not enough or too much fuel
- An attack on the software that manages barge scheduling or contracting, which could cause confusion and delay the barge
- An attack on the software or machines that provide fuel additives to convert Jet A fuel into military grade fuel, which could result in the wrong fuel mixture being sent to JBA
- An attack on the fuel quality sensors, which could prevent the identification of bad fuel at JBA, cause jets to receive bad fuel, and result in engines stalling out or corroding over time

This thesis focuses on applying the steps of the Moebius methodology to just the Colonial Pipeline and barge cyber-attacks for simplicity, but one could add more negative alternatives to the model or create separate models to explore different threats of interest. The ability to scale the number of alternatives in the model is one of the useful features of MP because it allows modelers to easily expand or contract their focus based on decision maker priorities or interest areas. It is important to have agreement on the intended

operation of the system, which negative alternatives to include, and the expected operation of those alternatives before assigning risk attributes.

C. STEPS 3–5: ADD RISK ATTRIBUTES AND CALCULATE OR ASSIGN IMPACT AND LIKELIHOOD VALUES

After completing the behavioral model, the next three steps of Moebius' methodology add attributes for risk in the form of likelihood and impact, and assign values to these attributes in the model. The Moebius methodology provides flexibility in choosing how to measure likelihood and impact in the model (Moebius 2018, 17). This section creates the likelihood values for the cyber-attack use cases, then it demonstrates two possible ways to model impact in MP: assessing multiple levels of a single type of impact using the example of schedule impact from the Colonial Pipeline cyber-attack; and modeling multiple types of impacts using a single value, or consequence factor, with examples from the barge cyber-attack. The section concludes by assigning values for impact and likelihood for both use cases in MP.

1. Likelihood Values

In the simple model for calculating risk, likelihood is a single value that represents both the likelihood of the attack occurring and the likelihood of the associated impacts occurring because of the attack (Smith and Merritt 2017, 21). Table 2 shows the likelihood values this thesis uses. The values range between zero, representing not likely to happen, and one, representing 90–100 percent likely to happen. There are only a handful of values available for the likelihood value to prevent decision makers from arguing over small differences (Smith and Merritt 2017, 79).

Table 1. Likelihood Values for Cyber-Attack Use Cases

Likelihood Value	Percent Likely to Occur
0	Not likely to occur
0.2	1-29% likely to occur
0.4	30-49% likely to occur
0.6	50-69% likely to occur

Likelihood Value	Percent Likely to Occur
0.8	70-89% likely to occur
1	90-100% likely to occur

Expert input or analysis would be the ideal source for assigning likelihood to the scenarios, but this thesis must draw from publicly available information, so the values in Table 1 are hypothetical ranges. Also, despite the numerical scale, the values are qualitative; they should not imply precision of measurement, especially in the risk calculations that add and multiply the values in subsequent steps.

2. Measuring Multiple Levels of Impact

MP offers several different options for measuring impact in the model. One way is by assessing how a specific behavior attribute changes as a result of different events occurring in the model. Consider the example of how long it takes fuel to flow through the jet fuel supply chain.

Figures 7, 8, 9, and 10 showed the MP model for the end-to-end jet fuel supply chain as it is intended to operate and how it would operate after a cyber-attack on the Colonial Pipeline causes light, medium, or heavy damage, respectively. The bar charts embedded in the figures reflect values assigned in the model code to quantify the impact of a cyber-attack on the total number of days JBA would not receive jet fuel due to damage to the Colonial Pipeline. Figure 13 shows those bar charts side-by-side for ease of comparison.

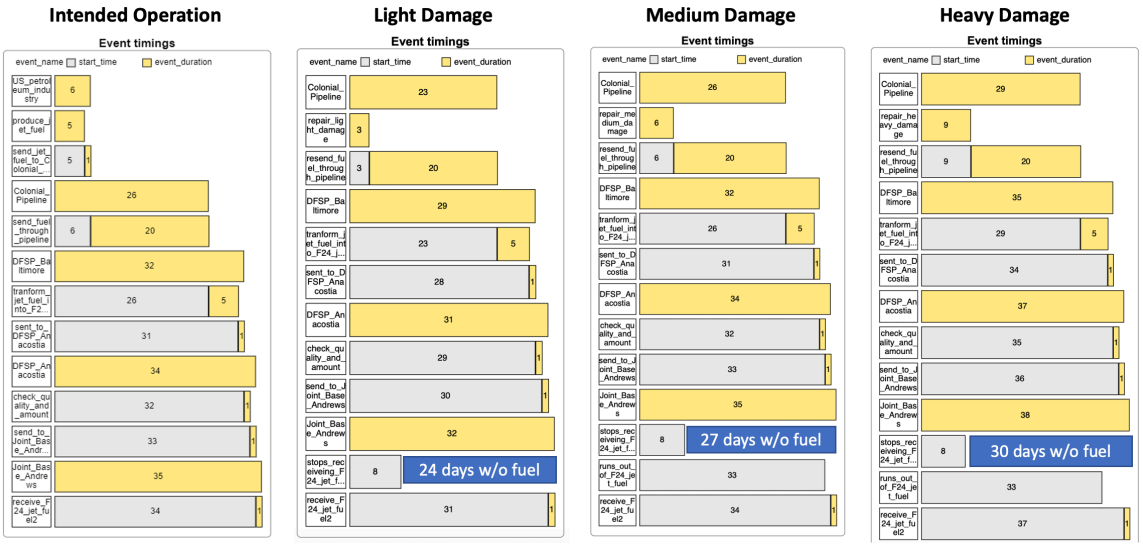

Figure 13. Comparison of the Range of Impacts on the Jet Fuel Supply Chain from a Cyber-Attack on the Colonial Pipeline. Source: Alden et al. (2020).

When the Pipeline operates as intended, Figure 13 shows it takes 20 days for fuel to transit the Pipeline. This duration appears in the intended operation bar chart under the bar titled send_fuel_through_pipeline, and in the other charts in the bar titled resend_fuel_through_pipeline. A cyber-attack on the Pipeline halts the flow of fuel until the Pipeline can be repaired. While the number of days to repair the Pipeline varies in each scenario, all scenarios assume JBA stops receiving fuel eight days after the cyber-attack occurs. The blue bar in each chart shows how many days JBA is without fuel as a result of the cyber-attack. For example, a cyber-attack with light damage takes notionally three days to repair. The Pipeline must then resend the jet fuel, which takes 20 days. Subsequent steps result in fuel taking a total of 32 days to transit from the Pipeline to JBA. Altogether, a cyber-attack with light damage results in a notional 24-day pause in JBA receiving jet fuel. An attack with medium damage notionally requires a six-day repair time, which causes a 27-day pause in JBA receiving jet fuel. An attack with heavy damage notionally causes a nine-day repair time, resulting in a 30-day pause in JBA receiving jet fuel.

The bar charts produced by the model allow decision makers to compare different levels of impact that could result from a cyber-attack. The bar charts display both the gap in time without fuel and the contributing factors underpinning those gaps. This insight can help decision makers develop different mitigation strategies. For example, MP shows that the degree of damage to the Pipeline results in different lengths of repair time, and those repair times result in different timelines for fuel stoppage at JBA. With that insight, decision makers can explore at least two paths for mitigations: mitigating the gap in fuel delivery, perhaps by keeping additional fuel reserves on base; and mitigating the root cause of the gap by finding ways to accelerate repair or replace time for the barge. MP not only helps visualize magnitude of impact, but it also helps decision makers understand contributing factors, which can better inform mitigation strategies.

3. Measuring Multiple Types of Impact

Schedule impact is only one type of impact a cyber-attack can have. The real-life cyber-attack on the Colonial Pipeline cost the Pipeline owners more than $4 million in ransom fees, and it impacted mission accomplishment by preventing citizens from obtaining the gas they needed to commute to work, reach goods and services, and enjoy recreation beyond walking distances. When multiple types of impacts could occur, decision makers must choose which aspects of impact they want to assess in the model.

If decision makers are interested in assessing more than one type of impact from a cyber-attack, one could create multiple models for the different types of impacts. Alternatively, Smith and Merritt (2017) provide several different techniques for calculating impact. One method they present creates a consequence factor, which is a single, dimensionless value that represents the presence of several impacts, a range of impacts, or both (Smith and Merritt 2017, 78). A consequence factor by itself can mask the underlying elements that contribute to risk, so it is important to provide transparency into the contributing elements via a table, diagram, or other description. It is also important, when aggregating impacts, to calibrate the factor to ensure reasonably consistent impacts across the different variables (Smith and Merritt 2017, 77). A consequence factor can be beneficial because it establishes agreed-upon trade-off rules

among different stakeholders (Smith and Merritt 2017, 28); for example, how decision makers should collectively value the relationship among cost, schedule, and performance impacts. By incorporating ranges of impact, the consequence factor can also prevent arguments over magnitude differences that do not matter (Smith and Merritt 2017, 29). It can be difficult to establish such a factor because it requires stakeholder consensus. Additionally, the numerical value of the consequence factor is not the same as a quantitative scale, so decision makers must be aware of how the factor translates into tangible impacts, especially when calculating and interpreting risk (Smith and Merritt 2017, 79–80). This thesis uses a consequence factor to measure the collective impact of a cyber-attack on cost, schedule, and performance elements of the jet fuel supply chain.

A consequence factor helps assess the multiple impacts a cyber-attack can cause. Consider the barge use case. The impact to schedule, cost, and mission performance are all relevant and important: if the barge is delayed or sunk, DOD could experience late fuel arrival, costs associated with replacing fuel lost on the sunk barge, and a reduction in the number of mission-capable jets available to defend the National Capital Region (NCR) due to fuel shortages. Instead of modeling and calculating these risks separately, a consequence factor helps understand the compound impact from schedule, cost, and mission performance.

Table 2 outlines the consequence factors this thesis uses to measure impact in the risk assessment. The table provides transparency into the cost, schedule, and performance elements that underpin the consequence factor. Similar to the likelihood values, there are only a handful of values available for the consequence factor to prevent decision makers from arguing over small differences (Smith and Merritt 2017, 79). These values range in odd increments from one to nine, representing lowest to highest impact, based on the expected cost, schedule, and performance impact of a barge delay or total loss. The data in Table 2 assume:

- There are 21 F-16 fighter aircraft in the 113th Wing on JBA (Heaton 2010).

- Each F-16 aircraft can carry 12,000 pounds (1,500 gallons) of fuel (U.S. Air Force 2015).
- Jet A fuel costs about $1.93 per gallon in North America (IATA 2021).
- The cost to refuel each F-16 aircraft is about $2,895 (1,500 gallons multiplied by $1.93 per gallon).
- The cost to refuel all fighter jets in the 113th Wing is about $60,795 ($2,895 per aircraft multiplied by 21 aircraft in the Wing).
- Not all the Wing's fighter jets need to be refueled at once because they support training and combat deployment missions in addition to standing alert to protect the NCR (Church 2012).
- It takes about 20 hours for a barge to go from Baltimore to Anacostia based on a 175 nautical mile trip from Baltimore, M.D. to Washington, D.C., (Cape Charles n.d.) and expected operating speed of a tugboat of about nine knots (Weeks Marine 2021).
- The cost for an additional barge to replace a delayed or sunk barge is about $7,620 (the approximate rate to move 88 metric tons of fuel (1,500 gallons per aircraft, multiplied by 21 aircraft in the Wing, divided by 358 gallons per metric ton) in the New York to Norfolk water corridor (Merlin Petroleum 2021).
- Costs associated with an attack on the Colonial Pipeline relate primarily to increased fuel prices that could result from the Pipeline being damaged and offline. For example, if Jet A fuel cost $2.50 per gallon, instead of $1.93 per gallon, the cost to refuel all the fighter jets in the 113th Wing would be $78,750. DOD would not fund repair of the Colonial Pipeline itself.

- Building upon the Colonial Pipeline cyber-attack use case, after eight days, JBA stops receiving fuel, so risk to schedule and mission performance is highest at, after, and leading up to an eight-day gap.
- All estimates for cost, schedule, and mission performance are notional, based on publicly available and often dated information, and would improve substantially if updated with expert input. For the purposes of this thesis, notional data are sufficient to demonstrate the functionality and benefits of using MP to model risk.

Table 2. Impact: Consequence Factors for Cyber-Attack Use Cases

Factor	Cost Impact	Schedule Impact	Performance Impact
1	<$10,000	<1 day delay	>85% jets are mission capable
3	$10,000 - $20,000	1-2 day delay	66-85% of jets are mission capable
5	$20,000 - $30,000	3-5 day delay	46-65% jets are mission capable
7	$30,000 – $50,000	6-8 day delay	25-45% jets are mission capable
9	>$50,000	>8 day delay	<25% jets are mission capable

4. Assigning Likelihood and Impact to the Use Cases

To calculate risk, each cyber-attack scenario receives a single value for likelihood and a single value for impact. Table 3 and Table 4 outline the likelihood and impact values for the two use cases in this thesis. The value for impact comes from the mean average of the individual consequence factors for cost, schedule, and performance. Table 3 shows the likelihood and impact assigned to the potential outcomes of the cyber-attack on the Colonial Pipeline. The most likely scenarios involving the Colonial Pipeline are cyber-attacks that require the Pipeline to repair light or medium damage. The scenarios where the Pipeline must repair medium or heavy damage have the highest impact factors of the outcomes in this use case.

Table 3. Likelihood, Impact, and Risk for Pipeline Cyber-Attack Use Case

Event & Outcome	**Like-lihood**	**Impact (Consequence Factor)**				**Risk Score**
		Cost Factor	Schedule Factor	Performance Factor	Final Factor	Likelihood * Impact
Do nothing	**0.2**	1	1	1	**1**	0.2
Repair light damage	**0.8**	7	9	7	**7**	5.6
Repair medium damage	**0.8**	9	9	7	**9**	7.2
Repair heavy damage	**0.6**	9	9	9	**9**	5.4

Table 4 shows the likelihood and impact assigned to the potential outcomes of the cyber-attack on the barge. The most likely scenario involving the barge is a cyber-attack that delays the barge. The delayed barge and the sunk barge share the highest impact factor of the outcomes in that use case.

Table 4. Likelihood, Impact, and Risk for Barge Cyber-Attack Use Case

Event & Outcome	**Likelihood**	**Impact (Consequence Factor)**				**Risk Score**
		Cost Factor	Schedule Factor	Performance Factor	Final Factor	Likelihood * Impact
No impact	**0.2**	1	1	1	**1**	0.2
Barge delayed	**0.8**	7	5	3	**5**	4
Barge sunk	**0.2**	9	3	3	**5**	1

Using a risk table, like Table 3 and Table 4, is useful at this stage for both the modeler and the decision maker. The risk tables provide transparency into the values underpinning each potential outcome of the use case. They also help modelers and decision makers visualize all the risk attribute values in one place and confirm the values before inputting them into the MP model. Once the values are in MP, SAY statements

can display these values alongside the sequence diagram that shows the context of the supply chain. The modeler can then compare the SAY statements to the risk tables to check the accuracy of the MP calculations and ensure the model is producing expected results.

5. Modeling Likelihood and Impact in MP

The final action to complete Steps 3–5 in the Moebius methodology is to write the MP code that assigns the values from Table 3 and Table 4 to attributes for likelihood and impact for each of the use case outcomes in the model. Figure 14 contains this MP code, extracted from the full model in the Appendix Section C. The ATTRIBUTES designation in the MP schema creates number variables for likelihood and impact, as well as for four variables (trace_risk_score, sum_risk_scores, max_risk_score, and max_risk_trace_unique_number) that the global calculation uses in Step 6. The COORDINATE statements in the MP schema assign likelihood and impact values according to those in Table 3 and Table 4.

```
ATTRIBUTES{number likelihood, impact, trace_risk_score, sum_risk_score,
                max_risk_score, max_risk_trace_unique_number;};

/* Assigns attributes for the Colonial Pipeline use case */

COORDINATE $no_pipe_attack: do_nothing
    DO  $no_pipe_attack.likelihood:= 0.2;
        $no_pipe_attack.impact:= 1;
    OD;

COORDINATE $attack_bursts_pipeline: repair_light_damage
    DO  $attack_bursts_pipeline.likelihood:= 0.8;
        $attack_bursts_pipeline.impact:= 7;
    OD;

COORDINATE $attack_bursts_pipeline: repair_medium_damage
    DO  $attack_bursts_pipeline.likelihood:= 0.8;
        $attack_bursts_pipeline.impact:= 9;
    OD;

COORDINATE $repair_complete_6days: repair_heavy_damage
    DO  $repair_complete_6days.likelihood:= 0.6;
        $repair_complete_6days.impact:= 9;
    OD;

/* Assigns attributes for the Barge use case */

COORDINATE $no_barge_attack: no_impact
    DO  $no_barge_attack.likelihood:= 0.2;
        $no_barge_attack.impact:= 1;
    OD;

COORDINATE $attack_to_delay: barge_delayed
    DO  $attack_to_delay.likelihood:= 0.8;
        $attack_to_delay.impact:= 5;
    OD;

COORDINATE $attack_to_destroy: barge_sunk
    DO  $attack_to_destroy.likelihood:= 0.2;
        $attack_to_destroy.impact:= 5;
    OD;
```

Figure 14. MP Code for Likelihood and Impact Attributes.

For completeness, Table 3 and Table 4 also show the risk score for each potential outcome, calculated by multiplying the values for likelihood and the final impact factor, but that calculation takes place in part of Step 6 in the Moebius methodology. The next section discusses the risk calculation in more detail.

D. STEP 6: USE IMPACT AND LIKELIHOOD TO CALCULATE, QUERY, AND SORT RISK

In Step 6, the Moebius methodology again gives decision makers flexibility by allowing them to choose their preferred way of mathematically calculating risk (Moebius 2018, 17). This flexibility is helpful because decision makers can calculate risk in the way most meaningful to their use case, and it allows this thesis to extend this step of the

Moebius methodology to include a global risk report in MP. This thesis calculates risk for each use case by multiplying the value for likelihood with the value for impact (i.e., the final consequence factor) per Table 3 and Table 4. To calculate the total risk in a model, this thesis adds together the risk scores for each use case in the model.

This section describes two examples of calculating risk in MP: a simple example using the barge cyber-attack, and a more complex example combining the Colonial Pipeline cyber-attack and the barge cyber-attack into one model to show how MP can calculate risk when there are two threats to the supply chain. Both examples generate a global report to assess risk across all the traces in the model. The addition of the global report extends Step 6 of the Moebius methodology. As a result, the title for this step is now, "Use Impact and Likelihood to Calculate, Query, and Sort Risk," instead of Moebius' original title, "Use Impact and Likelihood to Calculate Risk."

1. Simple Risk Calculation: Barge Cyber-Attack

The MP code for calculating risk as the product of likelihood and impact is quite simple. Figure 15 shows the MP code to display values for likelihood and impact, and calculate the risk score, for the barge cyber-attack use case. The full code for this MP model appears in the Appendix Section B. The COORDINATE statement tells the model to look in each trace for the key events in blue: no_impact, barge_delayed, and barge_sunk. If the trace contains any of these events, the SAY statements tell the model to display the words in orange and their values on the sequence diagram. The SAY statement for "Risk Score" tells MP to calculate the risk score as the product of the event likelihood and impact and then display that value on the sequence diagram.

```
/* Calculates risk and creates SAY statements for
Likelihood, Impact Factor, and Risk Score. */

COORDINATE $y: ( no_impact | barge_delayed | barge_sunk )
    DO
            SAY("Likelihood: "$y.likelihood);
            SAY("Impact Factor: "$y.impact);
            SAY("Risk Score: "$y.likelihood*$y.impact);

    OD;
```

Figure 15. MP Code to Calculate and Display the Risk Score.

Figures 16, 17, and 18 show the model results and display the risk score and the values for likelihood and impact using the values in Table 3 and Table 4.

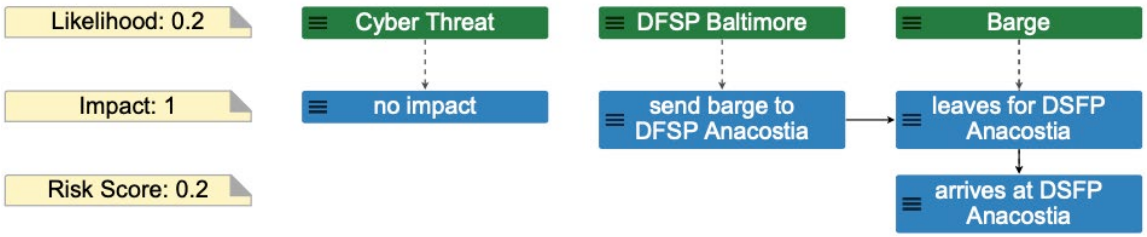

Figure 16. Cyber-Attack Has No Impact (Scope 1, Trace 3).

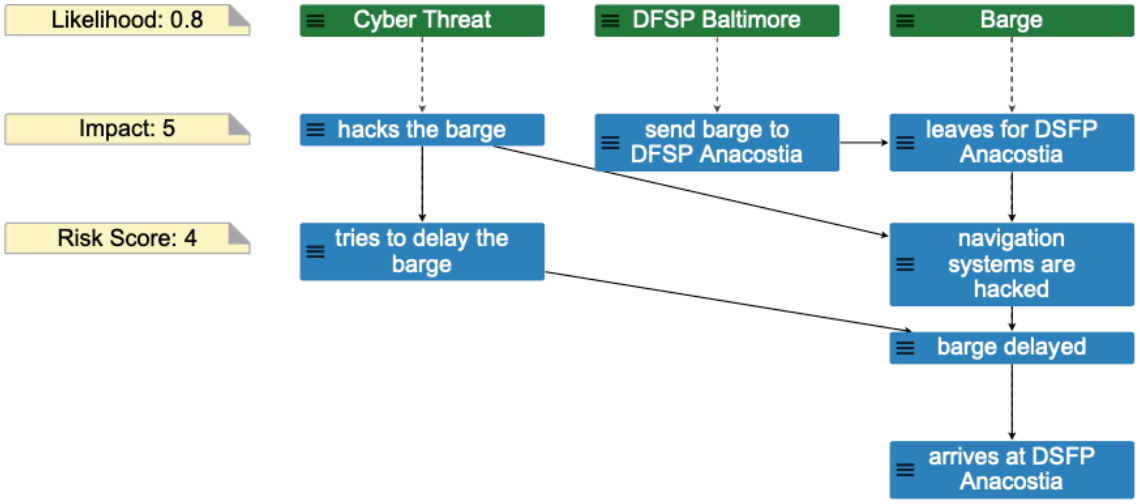

Figure 17. Cyber-Attack Delays the Barge (Scope 1, Trace 1).

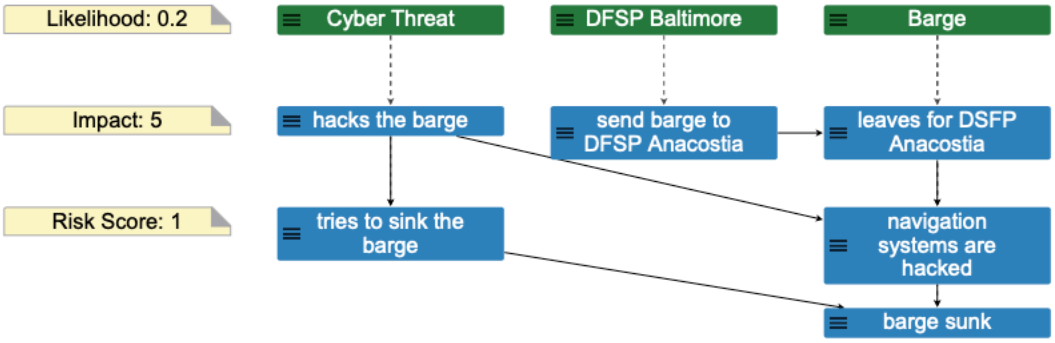

Figure 18. Cyber-Attack Sinks the Barge (Scope 1, Trace 2).

For this simple use case, with a small number of potential scenario outcomes and single values for likelihood and impact, MP generates only three traces. Manually reviewing the figures and ordering the traces by highest to lowest risk does not take much time. The scenario with highest risk is a cyber-attack that delays the barge (risk score of four), followed by a cyber-attack that sinks the barge (risk score of one), then a cyber-attack with no impact (risk score of 0.2). In more complex models, sorting and ordering becomes more difficult, so having an automated way to identify and categorize the traces could help humans focus on the traces that are most relevant to their areas of interest.

The global report provides this automation. This thesis is the first time the global report function has ever been applied to assessing risk. Figure 19 shows the MP code in the global section of the model for the cyber-attack on the barge. The code uses the attributes of likelihood, impact, trace_risk_score, sum_risk_scores, max_risk_score, and max_risk_trace_unique_number from Figure 14. It tells MP to perform several tasks:

- **Query Risk Across Scenarios to Enable Sorting**: Identify the maximum risk score (GLOBAL.max_risk.score) by going through each trace and comparing risk scores. If the current trace is higher than the last trace, update the maximum risk score to equal the highest value. Pull the number of the trace for the highest risk score (GLOBAL.max_risk_trace_unique_number) for inclusion in the global report. Mark all traces that have a risk score higher than a specific value (in this case, >=2) so the modeler can take advantage of the sort option in MP to have the marked traces appear at the top of the trace column.

- **Calculate Total Risk**: Add all the risk scores (GLOBAL.sum_risk.scores) to determine the total risk associated with the use case.

- **Calculate Average Risk**: Add all the risk scores and divide by number of traces (GLOBAL.sum_risk.scores/#$$TRACES) to determine the average risk across all use cases.

- **Create and Display a Global Risk Report**: State the title for the risk report and report the scope of the model. As part of the display, present the information in the SAY statements, including total risk across total number of traces, highest risk, average risk, and a direction to sort traces by those marked first.

Sort is a standard feature in MP. The menu is directly above the global report and it allows the user to sort event traces by those marked, by event number, or by probability. Probability in this case is not the same as the likelihood value in the model. Instead, it refers to the probability of the model generating a specific trace (Auguston 2020, 58). Modelers can assign specific conditions for event probability in the model; however, that feature of MP is outside the scope of this thesis.

```
/********************** GLOBAL Section *************************/

/*Sort Risk Across Scenarios*/

/*If the likelihood*impact for a given trace exceeds the current global maximum
risk factor value (initialized at zero), then make the max risk factor THIS
trace's risk factor and grab the trace id for the max risk trace.  */

        IF $y.likelihood*$y.impact > GLOBAL.max_risk_score THEN
            GLOBAL.max_risk_score:= $y.likelihood*$y.impact;
            GLOBAL.max_risk_trace_unique_number:= trace_id;
        FI;

            /*MARK traces that have a risk factor greater than a certain value.*/

            IF $y.likelihood*$y.impact >= 2 THEN MARK; FI;

/*Calculate Total Risk*/
        GLOBAL.sum_risk_scores +:= $y.likelihood*$y.impact;

    OD;

/*Create and Display Global Risk Report*/

/*Display a risk report before results of traces that includes:
total risk, highest risk, and average risk, and directions to sort traces by marked.*/

GRAPH risk_report{ };

GLOBAL
REPORT Global_Risk{TITLE("Risk Report for Scope " $$scope);};
WITHIN risk_report{ };

    SAY("Total risk over " #$$TRACE " traces: "
                                        GLOBAL.sum_risk_scores) => Global_Risk;
    SAY("Highest Risk: " GLOBAL.max_risk_score" at trace "
                                GLOBAL.max_risk_trace_unique_number) => Global_Risk;
    SAY("Average Risk: " GLOBAL.sum_risk_scores/#$$TRACE) => Global_Risk;

    SAY("Sort by Marked to view traces with a risk factor >= 2.") => Global_Risk;

    SHOW Global_Risk;

/***************************************************************/
```

Figure 19. MP Code for the Global Section with a Single Cyber Threat.

Figure 20 displays the model generated by adding the MP code in Figure 19. The global view with the global report appears in the top right corner of the model, above the list of traces MP generates. Traces are sorted with those marked appearing first.

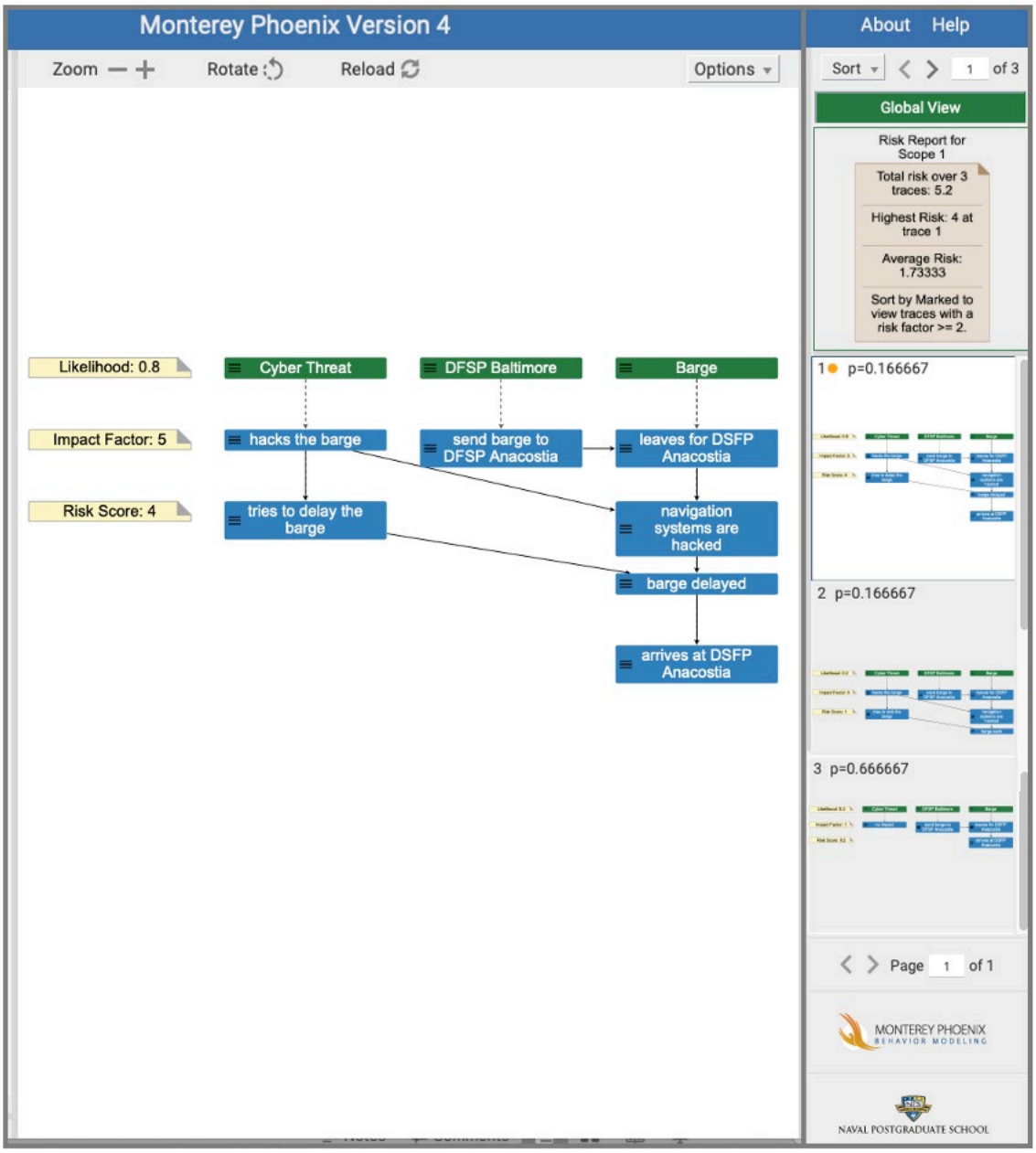

Figure 20. Global View in Upper-Right of MP Display for the Barge Cyber-Attack.

In Figure 20, the first trace is the only trace marked. It has an orange circle next to the trace number, which indicates the risk score is at or above the risk score threshold of two. No other traces were marked, so they have a risk score less than two. Two is an arbitrary number, chosen simply because it is the next highest whole number closest to the average risk across the traces (1.73). The modeler can easily change this number based on decision-maker risk tolerance or to support other view preferences. The purpose of the mark is so one can quickly determine which traces meet a risk tolerance level that is worth further investigation. In this case, the first trace is the only trace with above-average risk. The global report indicates the first trace is also the one with the highest risk score, so decision makers may want to discuss mitigations for this scenario—the cyber-attack that delays the barge—as a priority. The global view helps users quickly focus on and prioritize the scenarios of highest interest; then, users can click through the other traces to explore the other results.

2. Risk Calculation with Two Threats: Combined Attack Model

The automated calculations and display generated by the global report become increasingly useful when assessing risk in more complex use cases that generate numerous traces. Assume a decision maker has limited resources to invest in cyber security and wants to understand how to best allocate those resources to improve the security of the jet fuel supply chain. They need to assess and compare risk across multiple scenarios from multiple threats. To demonstrate this capability in MP, the author combined the MP models for the cyber-attack on the barge and the cyber-attack on the Colonial Pipeline. Figure 21 displays the resulting two-threat model using the scenario for its intended operation (i.e., each cyber threat has no impact on the intended operations of the supply chain). The code for this model appears in the Appendix Section C.

Figure 22 condenses the view from Figure 21 by hiding the nodes for DFSP Anacostia and JBA since there is no change to the events or impact at those nodes compared to scenarios included in earlier chapters of this thesis. MP allows the modeler to comment out this section of code to remove it from the display but keep it in the model. This technique preserves the completeness of the end-to-end supply chain model,

while simplifying information for decision makers so they can focus on only the aspects of the supply chain that are impacted by active cyber threats. The flexibility of MP allows modelers to customize the visual presentation for their audience while preserving the complete context of the system and its behavior.

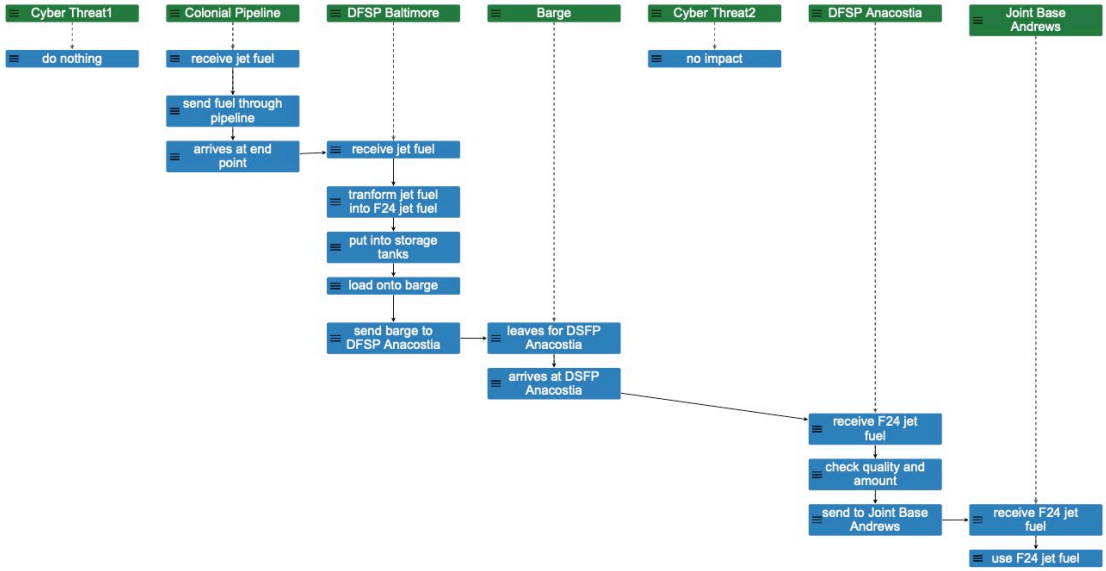

Figure 21. MP Model of Two Cyber Threats to the Jet Fuel Supply Chain (Scope 1, Trace 12).

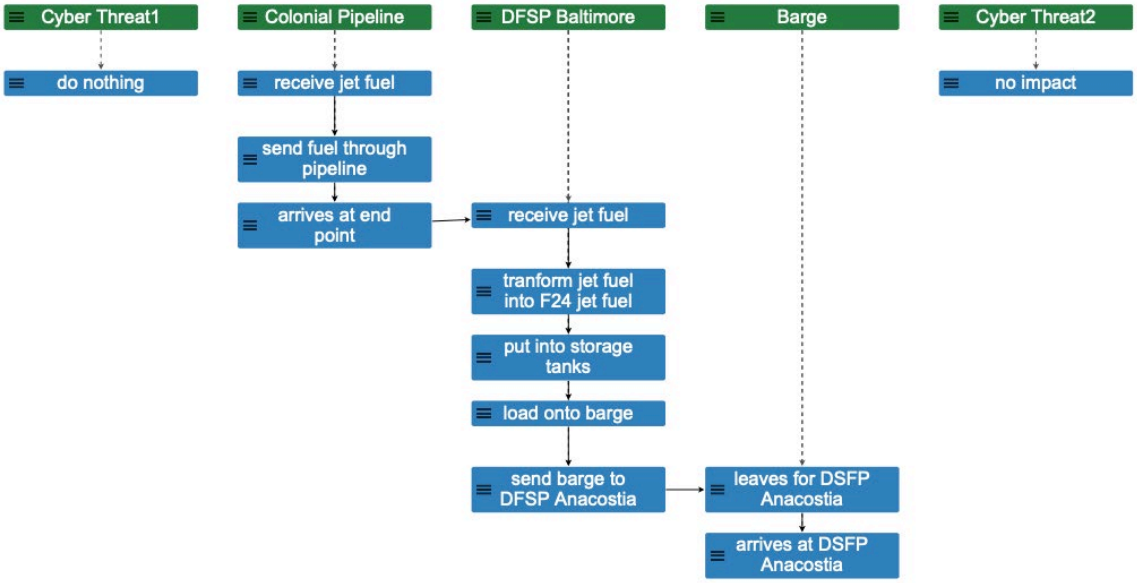

Figure 22. Condensed MP Model with Two Cyber Threats to the Jet Fuel Pipeline (Scope 1, Trace 12).

The MP model with two cyber threats includes the same outcomes and associated likelihood and impact factors for the Colonial Pipeline and barge cyber-attacks described in Table 3, Table 4, and Figure 14. It also includes a global report similar to that contained in the barge model in Figure 19; however, the presence of multiple threats in the model requires an adjusted approach to calculating and querying risk. Figure 23 shows the MP code in the global section of the model with two cyber threats. There are two differences in this model compared to the model that had only one cyber threat:

- **Multiple Variables to Calculate Risk**: The two-threat model includes two different variables—one for each use case—to calculate risk. There is an outer COORDINATE function (COORDINATE $y) to calculate risk across the Colonial Pipeline cyber-attack use case, and an inner COORDINATE function (COORDINATE $z) to calculate risk across the barge cyber-attack use case. Including a separate variable for each use case allows the model to calculate and display the risk associated with that use case, as well as perform a separate calculation for the total risk to the supply chain from both cyber threats.

- **Trace_Risk_Score**: Because there are multiple risk calculations, the two-threat model introduces a new attribute, trace_risk_score, which adds together the risk from each use case to generate the total risk to the supply chain from both cyber threats. Trace_risk_score replaces the risk variable ($y.likelihood*$y.impact) where it appeared in the global report section of the simple model. A simple model with only one cyber threat, like the barge cyber-attack, has the option of using the trace_risk_score variable or directly calculating risk ($y.likelihood*$y.impact). Once the number of threats is greater than one, using trace_risk_score is how MP knows to store the results of the risk calculations from different threats separately when they appear in the same trace. That way, decision makers can compare the risk across different threats.

Apart from these two changes, the two-threat model functions as previously described: it marks traces above a certain threshold value and issues a risk report that contains the total risk across the total number of traces, highest risk, average risk, and a direction to sort traces by those marked first.

```
/**********Global Risk Section**********/

/*Calculate Risk Across Scenarios*/

/*OUTER COORDINATE GETS PIPELINE CONTRIBUTION TO RISK*/
COORDINATE $y: ( do_nothing | repair_light_damage | repair_medium_damage | repair_heavy_damage)

    /*INNER COORDINATE GETS BARGE CONTRIBUTION TO RISK*/
    DO COORDINATE $z: ( no_impact | barge_delayed | barge_sunk )
        DO

        /*GET THE TOTAL RISK SCORE FOR EACH TRACE (PIPELINE + BARGE)*/
        trace_risk_score+:= ($y.likelihood*$y.impact) + ($z.likelihood*$z.impact);

        /*Display risk attributes for the scenario*/
        SAY("Pipeline Likelihood: "$y.likelihood", Pipeline Impact: "$y.impact", Pipeline Risk Score: "$y.likelihood*$y.impact);
        SAY("Barge Likelihood: "$z.likelihood", Barge Impact: "$z.impact", Barge Risk Score: "$z.likelihood*$z.impact);


/*Sort results*/

        /*If the TRACE RISK SCORE for a given trace exceeds the current global maximum
        risk factor value (initialized at zero), then make the max risk factor THIS
        trace's risk factor and grab the trace id for the max risk trace.  */

        IF  trace_risk_score > GLOBAL.max_risk_score THEN
            GLOBAL.max_risk_score:= trace_risk_score;
            GLOBAL.max_risk_trace_unique_number:= trace_id;
        FI;

            /*MARK traces that have a risk factor greater than a certain value*/

            IF trace_risk_score >= 6.34 THEN MARK; FI;
        OD;
    OD;


/*Calculate Total Risk*/

/*Sum up risk scores across all traces*/
GLOBAL.sum_risk_score +:= trace_risk_score;

    /*ADD THE TOTAL RISK FOR EACH TRACE (PIPELINE + BARGE)*/
    SAY("Total Trace Risk: "trace_risk_score);


/*Create and Display Global Risk Report*/

GLOBAL
REPORT Global_Risk{TITLE("Risk Report for Scope " $$scope);};

/*Include these SAY statements in the Global_Risk REPORT. */
SAY("Total risk over " #$$TRACE " traces (sum of trace risk scores): "
                                    GLOBAL.sum_risk_score) => Global_Risk;
SAY("Highest Risk: " GLOBAL.max_risk_score" (trace "
                                GLOBAL.max_risk_trace_unique_number")") => Global_Risk;
SAY("Average Risk: " GLOBAL.sum_risk_score/#$$TRACE)
    => Global_Risk;
SAY("Sort by Marked to view traces with above average risk >=6.34.") => Global_Risk;

SHOW Global_Risk;
```

Figure 23. MP Code for the Global Section with Two Cyber Threats.

Before discussing this use case further, it is important to note two limitations of this model: it is not scalable to more than two threats, and it requires the “y” and “z” events specified in the nested COORDINATE statements to appear only once in each trace and be mutually exclusive. The two cyber threats in the jet fuel supply chain use case meet these conditions, so the model is accurate; however, more complex models that contain more than two threats or the iteration of one or more processes need a different approach to calculating risk. An example of an alternative approach is in the Appendix Section D. It produces the same results as the MP code in Figure 23, but is scalable to more than two threats and processes with iterative steps. The model limitations and the adjusted code in Section D evolved while validating the model. It would be beneficial to further test and validate this code on use cases with more than two threats; however, that

is outside the scope of this thesis. For the purposes of demonstrating the ability of MP to help decision makers assess, visualize, and prioritize cyber threats, this thesis will use the two-threat model in Figure 23. Figure 24 shows the visualization generated by that MP code, including the global report and the trace with the highest risk.

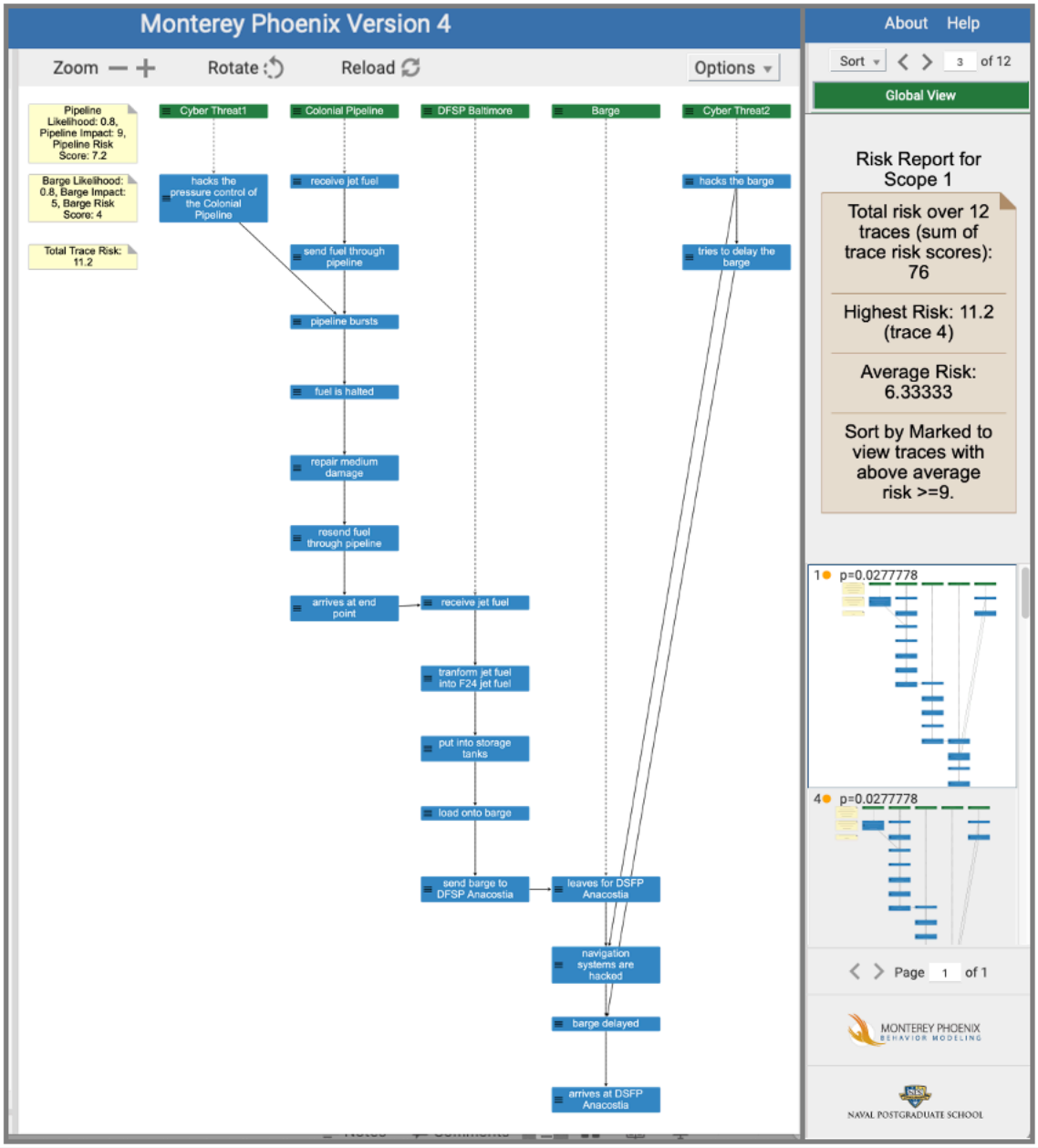

Figure 24. Highest Risk Trace in Model with Two Cyber Threats (Scope 1, Trace 4).

The jet fuel supply chain model with two cyber threats shown in Figure 24 produced a total of 12 traces, four times more than the barge model, which had only one cyber threat and produced three traces. As the number of threats or potential scenario outcomes increases, it becomes harder to manually sort through the results of the model to identify the traces of greatest interest. The global report is especially useful in these more complex models because it calls attention to the traces that meet a specific threshold for risk. For example, at the top right of the screen, the global risk report indicates the trace with the highest risk is trace four with a risk score of 11.2. After sorting by marked traces, one can quickly find trace four and see the sequence diagram that explains the scenario: a cyber-attack on the Colonial Pipeline required repairs to medium damage and a cyber-attack on the barge navigation systems delayed the barge. Together, these events create the highest risk to the supply chain's intended operations.

To see how other scenarios compared to the one with highest risk, decision makers can go back to the list of sorted traces. The list quickly shows there are only two other traces with a risk score of nine or higher. Nine was the threshold for marking traces in this model because, on the first run of the model, seven of the 12 total traces generated had a risk score higher than the 6.34 average. After stratifying the total risk from highest to lowest across those seven traces (11.2, 9.6, 9.4, 8.2, 7.4, 6.6, 6.4), revising the threshold to nine reduced the number of scenarios to explore in the initial review. Changing the threshold value for marking took only a few seconds to update in the code, re-run, and display. The agility of MP to respond so quickly to updates in the model is a key benefit of the tool. It could even allow decision makers to run excursions in the meeting room, if desired, and avoid unnecessarily postponing decisions to a later meeting just to make simple changes to model assumptions.

The global report adds additional analytic capability to risk assessment in MP, and it extends the Moebius methodology by providing decision makers an automated way to summarize, compare, and sort the results of multiple traces. This is especially useful in more complex models that have multiple cyber threats and generate numerous traces that take humans more time to evaluate than machines. With risk calculated, queried, and

sorted in this extended Step 6, there is only one more step to complete the methodology: displaying results to decision makers.

E. STEP 7: OUTPUT DESIRED FORMAT OF RISK FOR DECISION MAKER

The Moebius methodology allows modelers to tailor how to communicate risk to decision makers so it best meets their needs (Moebius 2018, 18). The literature review of this thesis explored traditional ways DOD displays risk—in a risk table, risk map, or risk matrix—and how features in MP improve upon those traditional displays. The sequence diagram in MP, timetables, SAY statements, and global report provide useful visualizations of risk that decision makers can easily understand and interact with in real time. This section uses the two-threat cyber-attack model to discuss the benefits of sharing MP visualizations directly with decision makers.

The visualization of the two-threat MP model, shown in Figure 24, is an information-rich but easy to understand display. The sequence diagram shows the context of how the jet fuel supply chain functions by describing the key nodes and events in the supply chain. It helps decision makers visualize exactly where the cyber-attack is coming from, what nodes it impacts, and what events it causes. Displaying the sequence diagram to decision makers ensures they have a shared understanding of how the system works and the various scenarios that introduce risk. This baseline of understanding can be helpful at overcoming organization stovepipes, especially when bringing together decision makers from different organizations with varying levels of knowledge about the system. Additionally, decision makers can be confident the various scenarios represent all possible outcomes within the model scope, so there are no unknown risks they might be missing.

The global report on the top right of Figure 24 displays the total risk and the average risk across all scenarios. If decision makers had to choose how to prioritize risk among multiple supply chains—such as jet fuel, parts, food, people, or more—they would be able to quickly compare the global reports from each supply chain model in MP. The global report also identifies the risk threshold for marking traces. Once sorted,

decision makers can quickly see across the 12 possible scenarios that MP identified only three traces with risk higher than nine. As they explore those three highest-risk traces first, they would see from the sequence diagram that all three scenarios included a cyber-attack on the Colonial Pipeline, but only two of the three traces included a cyber-attack on the barge navigation systems that had an impact. These results could suggest the vulnerability of the Colonial Pipeline to cyber-attack presents greater risk to the jet fuel supply chain than the vulnerability of the barge to cyber-attack. If limited resources are available to mitigate vulnerabilities in the supply chain, decision makers could choose to prioritize mitigations that reduce the likelihood or impact of an attack on the Colonial Pipeline over mitigations for the barge.

If decision makers are uncomfortable basing a mitigation strategy on only the three highest risk scenarios, modelers can easily change the threshold for marking traces and quickly rerun the model. Decision makers could then see additional scenarios for how one or both cyber-attacks impact the supply chain. Alternatively, if decision makers have "what if" questions that require changing likelihood or impact values, modelers can easily update the MP code and quickly rerun the model to demonstrate the impact of the change.

Using MP for both analyzing and displaying information to decision makers offers additional context and insight compared to traditional tools like the risk table, risk map, and risk matrix. Decision makers will likely need a variety of different visuals to support their assessment and prioritization of risk, but the displays MP provides offer rich context and insight on the system and potential risks. MP provides a common framework for understanding how the jet fuel supply chain works, transparency into the thinking and data underpinning the risk assessments, an exhaustive set of scenarios with risks from cyber-attack, and an agile tool that can address "what if" questions easily and quickly. These features of MP allow decision makers to have more substantive debate on, or justification for, their decisions.

V. CONCLUSIONS

The research question this thesis sought to answer was how can decision makers use MP to assess, visualize, and prioritize cyber risk in a supply chain? This section summarizes the conclusions of this research and identifies areas that would benefit from additional research.

There are four main conclusions of this research. First, the Moebius methodology (2018) is repeatable and extendable. There is enough rigor in the methodology to guide a modeler through using MP to assess risk, and enough flexibility for the modeler to tailor the model variables, risk calculations, and display output to their use case and decision-maker needs. This thesis successfully applied the Moebius methodology to a supply chain use case and built models for single-threat and two-threat use cases. It also extended the methodology by modifying the global report to support risk assessment for the first time, including using new calculations for total risk, average risk, and a risk threshold for marking traces.

Second, MP allows decision makers to achieve and assess a common understanding of how the supply chain works end-to-end, and how cyber threats could impact different aspects of the supply chain. This thesis demonstrated a model for a cyber-attack that disrupted the entire supply chain. That model included a timeline to understand the impact of an attack on fuel delivery gaps at JBA. This thesis also dissected a single part of the supply chain—the barge—to understand the risk from a cyber-attack to operations in that specific part of the supply chain. The simple barge model demonstrated the utility of being able to break down a complex system into smaller parts to facilitate better understanding of how various nodes function, interact, and change as the result of adding negative alternatives. This thesis also included a model with two cyber threats to the supply chain to understand the risk associated with different combinations of cyber-attacks.

MP has the capability and capacity to support risk assessments on broad and narrow aspects of the supply chain, so modelers can tailor their work in MP to explore

the areas of greatest interest to decision makers. Tailoring the model can help decision makers resolve differences in knowledge, assumptions, and perspectives. The model forces decision makers from different organizations and backgrounds to agree on a common definition of how the system operates and how negative alternatives might alter the intended operation. Creating a tailored model to explore a specific aspect of system behavior that decision makers might disagree on can help facilitate discussion and ideally resolve disagreements.

Third, the benefit of using MP to assess risk increases as use cases grow in complexity. For example, consider the simple barge model, which generated only three scenarios in its risk assessment, compared to the two-threat model that generated 12 potential scenarios. MP automatically generated the 12 traces in less than one minute, which is hours or days faster than humans could have brainstormed and created the same number of traces in a SysML model. Decision makers can also have confidence that the scenarios MP generates are exhaustive within the scope of the model, so there are no blind spots: the model includes all possible scenarios and not just those humans were able to conceptualize. Additionally, instead of manually reviewing and sorting all 12 traces, the global report on risk helped decision makers quickly identify the total and average risk across all the traces. The report marked traces with risk scores that met the user-defined threshold level, and then the sort function in MP presented the traces by those marked first. The marked traces help decision makers quickly orient to the scenarios that met their defined threshold of interest, allowing more time for discussion on mitigation strategies and less time sorting through model results.

Finally, MP provides the ability to visualize risk more comprehensively than existing risk assessment tools. The risk table, risk map, and risk matrix have limitations in how they communicate the context of the system, interdependencies among risks, static data that cannot be manipulated for real-time "what if" drills, and aggregate risk. MP has features that can overcome these limitations.

- **Context**: MP gives decision makers the ability to calculate and visualize risk in the context of the full system, with all scope-complete scenarios exposed. The sequence diagram in MP helps decision makers visualize the

flow of events within and among the supply chain nodes and communicates important context about the system and its environment, including order and precedence, cause and effect, people and places, and behavior attributes like timing, cost, performance, and personnel. This information creates shared understanding among decision makers from different backgrounds on how the system operates and what factors generate risk to the system. A common baseline is especially helpful when trying to achieve agreement among decision makers from different organizations that have different roles in, and views of, the supply chain. Decision makers can use the modeling process, and the approachable visualizations it produces, to achieve a shared view of the situation upon which they can then base their debates, decisions, and justifications.

- **Interdependencies**: The sequence diagram in MP also communicates interdependencies that exist among events and risks in the system. For example, the timetable bar charts created in the Colonial Pipeline model displayed the gap in time JBA went without fuel and the events that contributed to those gaps. The charts showed Pipeline repair time as the primary driver of the fuel delivery gap since the Pipeline required 20 days to reflow fuel after the repair regardless of the length of repair time. Decision makers could choose to prioritize mitigations that reduce repair time or those that give JBA access to an alternative supply of fuel since they cannot shorten the 20-day fuel transit time through the Pipeline. Understanding interdependencies can help decision makers develop different mitigation strategies, perhaps prioritizing contributing factors that address the root cause of a vulnerability over addressing more visible symptoms of an attack.

- **Responsiveness**: Too often, decision makers must delay a decision because the analysis underpinning the recommended course of action is not within the risk assessment presentation and analysts need to go back to

their desks to update calculations and summary charts in response to questions about what might occur if there were changes in certain assumptions or variables. With MP, modelers can easily update the assumptions and variables in the model and quickly rerun the simulation in seconds to regenerate scenarios and risk assessments. The speed of recalculation is so fast that MP could be used in the meeting room with decision makers to answer "what if" questions in real time. The interactive environment of MP provides a tool that could make meetings about risk prioritization more interactive and productive, and decisions more timely.

- **Aggregate Risk**: The addition of the global report to risk assessment in this thesis adds more valuable information to the standard MP display. The global report calculates risk across all scenarios and summarizes it in a concise report in the top right of the MP display. This information includes values for aggregate risks, like total risk and average risk across all scenarios.

The package of features in MP is not available in existing risk assessment approaches, yet analysts and decision makers are not using MP widely for risk assessment today. One reason may be lack of awareness. The Moebius methodology exists in a thesis with distribution restricted to DOD and DOD contractors only (Moebius 2018). This thesis has unlimited distribution with the intent of sharing the Moebius methodology, along with the extensions to the methodology described herein. The author hopes this thesis will inform analysts and decision makers about the ways in which they can use MP models to better assess and prioritize risk, especially the risk associated with cyber-attack on a supply chain. To that end, the code for the single-threat and two-threat models used in this thesis, as well as the model in the Appendix Section D that has an alternative risk calculation and query approach for more complex use cases, should be available on the MP-Firebird website so others can reuse and improve upon the models. More research should also be done to expand the use and maturity of MP for risk assessment.

Modeling risk in MP, especially supply chain risk, is still nascent research. Future research should improve upon the quality and type of assessments MP can do, the visualizations it creates to support decision makers, and the ability of the modeling software to handle more complex use cases. Specifically, future work could develop MP models that incorporate more risk assessment best practices. For example, this thesis used the simple model for evaluating risk, which has one variable each for likelihood and impact. Further research could create the MP code for the standard risk model, which is a better estimator of risk (Smith and Merritt 2002, 25). The creation of additional MP models could also incorporate events with different impact measures (i.e., cost, schedule, and performance attributes) instead of using a consequence factor. It could also evolve the code for the global report to account for different impact measurements. Future work should also test and validate the alternative approach to risk calculation and query, contained in the model in the Appendix Section D, on use cases with more than two cyber threats and iterative processes to refine how MP assesses and displays risk in more complex use cases. It could additionally incorporate risk mitigation actions into the model and test how the risk assessment changes in response to the addition of countermeasures.

Future work could also include research that informs DOD and other agency policies and practices. Research could do a more detailed comparison of the way MP assesses and visualizes risk compared to existing DOD tools, especially the risk matrix. It could make recommendations for how DOD could evolve its approach to risk assessment, including by incorporating MP models into risk management activities. Future research, or actual risk assessment practitioners, could also use MP to conduct a real-world risk assessment, with subject matter expert input and decision maker feedback, to assess the utility of the model and approach compared to existing tools. Feedback from real practitioners on real examples would be very valuable in informing how to best evolve MP to support analysts and decision makers responsible for managing risk.

At a time when the idea of a cyber-attack on the jet fuel supply chain is not just an academic excursion, but a real-world headline, there is an urgent need for more intuitive, interactive, and responsive tools to support decision makers. The extended Moebius

methodology with the global report, and the single-threat and two-threat use case baseline models, now exist with unlimited distribution so analysts and decision makers can explore risk in more comprehensive ways than current tools allow. It is the author's hope that decision makers will recognize the opportunity MP provides to enhance risk assessment and employ the tool—not just at the analyst console, but in the board room—to secure critical systems, infrastructure, and supply chains from future cyber-attack.

APPENDIX. MONTEREY PHOENIX CODE

This section contains the MP software code associated with the models in this thesis. Each section corresponds to a model used in this thesis, organized by order of appearance in the document.

A. MP CODE FOR JET FUEL SUPPLY CHAIN USE CASE

This MP software code is for the model developed by the team of NSA interns to demonstrate the impact of a cyber-attack on a military jet fuel supply chain (Alden et al. 2020).

```
/*
Model about a Jet Fuel Supply Line
Created on 6/15/2020-7/5/2020
By Nathaniel Alden
With help from Rachel Talkington

Update 1.1     Added a Gantt Chart
6/16/2020
Update 1.2     Tested a new way of way of making Gantt Chart in an attempt
6/17/2020    to increase readability. May become untenable as the model is expaned.
Update 1.3     Corrected root name error for JBA in durations setting.
6/18/2020    Removed redundecy in event duration setting.
             Replaced unused DLA Energy Root with Cyber Threat Root.
             Added attack and repair events.
             Changed Gantt Chart timing to start right after the attack.
             Added event for when JBA stops receiving fuel left in Supply Line after attack.
             Removed old code from 1st Gannt Chart attempt.
             Added Say statements to describe events
Update 1.4     Changed the Gannt Chart for events when no attacks happen to start at the refinery
6/21/2020    Created one place in the code for Say annotations and moved previous annotations there
             Added new annotations explaining the events and traces
             Added fuel use logic needs expanding.
             Added ENSURE statment instead of COORDINATE for the runs out of jet fuel event
*/
/**/

SCHEMA Supply_Line


/**/
ROOT US_petroleum_industry:
    produce_jet_fuel
    send_jet_fuel_to_Colonial_Pipeline
;
/**/
ROOT Colonial_Pipeline:
    receive_jet_fuel1
    send_fuel_through_pipeline
    [
        pipeline_bursts
        fuel_is_halted
        (
            repair_light_damage |
            repair_medium_damage |
            repair_heavy_damage
        )
        resend_fuel_through_pipeline
    ]
    arrives_at_end_point
;
/**/
COORDINATE    $x: send_jet_fuel_to_Colonial_Pipeline     FROM US_petroleum_industry,
            $y: receive_jet_fuel1 FROM Colonial_Pipeline
    DO ADD $x PRECEDES $y; OD;
/**/
ROOT Cyber_Threat:
    (
        hacks_the_pressure_control_of_the_Colonial_Pipeline |
        do_nothing
    )
;
```

```
;
/**/
COORDINATE    $x: hacks_the_pressure_control_of_the_Colonial_Pipeline     FROM Cyber_Threat,
              $y: pipeline_bursts FROM Colonial_Pipeline
    DO ADD $x PRECEDES $y; OD;
/**/
ROOT  DFSP_Baltimore:
    receive_jet_fuel2
    tranform_jet_fuel_into_F24_jet_fuel
    put_into_storage_tanks
    load_onto_barge
    sent_to_DFSP_Anacostia
;
/**/
tranform_jet_fuel_into_F24_jet_fuel:
    {
        add_iceing_inhibitor,
        add_static_dissipater,
        add_corrosion_inhibitor
    };
/**/
COORDINATE    $x: arrives_at_end_point     FROM Colonial_Pipeline,
              $y: receive_jet_fuel2 FROM DFSP_Baltimore
    DO ADD $x PRECEDES $y; OD;
/**/
ROOT  DFSP_Anacostia:
    receive_F24_jet_fuel1
    check_quality_and_amount
    send_to_Joint_Base_Andrews
;
/**/
COORDINATE    $x: sent_to_DFSP_Anacostia     FROM DFSP_Baltimore,
              $y: receive_F24_jet_fuel1 FROM DFSP_Anacostia
    DO ADD $x PRECEDES $y; OD;
/**/
ATTRIBUTES{number     fuel_reserves, fuel_use_perday;};

ROOT Joint_Base_Andrews:
    use_F24_jet_fuel
    [
        stops_receiveing_F24_jet_fuel
        [
            runs_out_of_F24_jet_fuel
           /* [ receives_F24_jet_fuel_from_other_bases ] */
        ]
    ]

/**/
    receive_F24_jet_fuel2
;
/* Arbitrary units are used */
COORDINATE     $jba: Joint_Base_Andrews
    DO
        $jba.fuel_reserves:= 25;
        $jba.fuel_use_perday:= 1;
    OD;

/**/
COORDINATE    $x: send_to_Joint_Base_Andrews     FROM DFSP_Anacostia,
              $y: receive_F24_jet_fuel2 FROM Joint_Base_Andrews
    DO ADD $x PRECEDES $y; OD;
/**/
COORDINATE    $x: fuel_is_halted     FROM Colonial_Pipeline,
              $y: stops_receiveing_F24_jet_fuel FROM Joint_Base_Andrews
    DO ADD $x REMAINING_FUEL_REACHES_END_OF_SUPPLY_LINE $y; OD;

/*GanttChart*/

/*Colonial_Pipeline_Durations*/
IF #do_nothing > 0 THEN
    COORDINATE     $p: send_fuel_through_pipeline
        DO
            SET $p.duration AT LEAST 20;
        OD;
FI;

IF #hacks_the_pressure_control_of_the_Colonial_Pipeline > 0 THEN
    COORDINATE     $p: resend_fuel_through_pipeline
        DO
            SET $p.duration AT LEAST 20;
        OD;
FI;

IF #repair_light_damage > 0 THEN
    COORDINATE    $p: repair_light_damage
        DO
            SET $p.duration AT LEAST 3;
        OD;
FI;

IF #repair_medium_damage > 0 THEN
    COORDINATE    $p: repair_medium_damage
        DO
            SET $p.duration AT LEAST 6;
        OD;
FI;

IF #repair_heavy_damage > 0 THEN
    COORDINATE    $p: repair_heavy_damage
        DO
            SET $p.duration AT LEAST 9;
        OD;
FI;

/*DFSP_Baltimore_Durations*/
COORDINATE     $b: DFSP_Baltimore,
              $b2: tranform_jet_fuel_into_F24_jet_fuel,
              $b3: sent_to_DFSP_Anacostia
    DO
        SET $b2.duration AT LEAST 5; /*Undisclosed amount of time*/
        SET $b3.duration AT LEAST 1;
    OD;
```

```
/*DFSP_Anacostia Durations*/
COORDINATE      $a: check_quality_and_amount,
                $a1: send_to_Joint_Base_Andrews
    DO
        SET $a.duration AT LEAST 1;
        SET $a1.duration AT LEAST 1;
    OD;

/*Joint_Base_Andrews Durations*/
COORDINATE $jba: receive_F24_jet_fuel2
    DO
        SET $jba.duration AT LEAST 1;
    OD;

IF #fuel_is_halted > 0 THEN
    COORDINATE
            $jba: stops_receiveing_F24_jet_fuel,
            $p: Colonial_Pipeline,
            $a: DFSP_Anacostia
        DO
            SET $jba.start AT LEAST $a.duration - $p.duration;
        OD;
FI;
/*fuel use logic*/
IF #hacks_the_pressure_control_of_the_Colonial_Pipeline > 0
THEN
    COORDINATE
        $jba: Joint_Base_Andrews,
        $f: receive_F24_jet_fuel2,
        $g: stops_receiveing_F24_jet_fuel
        DO
            IF $jba.fuel_reserves / $jba.fuel_use_perday < $f.end-$g.start
            THEN
                ENSURE #runs_out_of_F24_jet_fuel > 0;
                COORDINATE    $y: runs_out_of_F24_jet_fuel     FROM Joint_Base_Andrews
                    DO
                        SET $y.start AT LEAST $g.start+($jba.fuel_reserves / $jba.fuel_use_perday);
                    OD;
            ELSE
                ENSURE #runs_out_of_F24_jet_fuel < 1;
            FI;
        OD;
FI;
/**/

TABLE Time_table{ TITLE("Event timings");
        TABS string event_name,     number start_time,
             number event_duration;
   };
CLEAR Time_table;

IF #hacks_the_pressure_control_of_the_Colonial_Pipeline > 0
THEN
    COORDINATE $x: (
        Colonial_Pipeline |
        resend_fuel_through_pipeline |
        repair_light_damage |
        repair_medium_damage |
        repair_heavy_damage |
        DFSP_Baltimore |
        tranform_jet_fuel_into_F24_jet_fuel |
        sent_to_DFSP_Anacostia |
        DFSP_Anacostia |
        check_quality_and_amount |
        send_to_Joint_Base_Andrews |
        Joint_Base_Andrews |
        stops_receiveing_F24_jet_fuel |
        runs_out_of_F24_jet_fuel |
        receive_F24_jet_fuel2

        )     DO
        Time_table <|     event_name:     SAY($x),
                        start_time:     $x.start.smallest,
                        event_duration: $x.duration.smallest;
        OD;
ELSE
    /*US_petroleum_industry*/
    COORDINATE
            $r: US_petroleum_industry,
            $r2: produce_jet_fuel,
            $r3: send_jet_fuel_to_Colonial_Pipeline
    DO
        SET $r2.duration AT LEAST 5;
        SET $r3.duration AT LEAST 1;
    OD;
    COORDINATE $x: (
        US_petroleum_industry|
        produce_jet_fuel |
        send_jet_fuel_to_Colonial_Pipeline |
           Colonial_Pipeline |
        send_fuel_through_pipeline |
        DFSP_Baltimore |
        tranform_jet_fuel_into_F24_jet_fuel |
        sent_to_DFSP_Anacostia |
        DFSP_Anacostia |
        check_quality_and_amount |
        send_to_Joint_Base_Andrews |
        Joint_Base_Andrews |
        receive_F24_jet_fuel2
        )     DO
        Time_table <|     event_name:     SAY($x),
                        start_time:     $x.start.smallest,
                        event_duration: $x.duration.smallest;
    OD;
FI;
```

```
SHOW Time_table;

BAR CHART Timing{ TITLE("Event timings");
    FROM Time_table;
    X_AXIS event_name;
    TABS start_time, event_duration;
    ROTATE;
};

SHOW Timing;

/*Say annotations */
IF #hacks_the_pressure_control_of_the_Colonial_Pipeline > 0 THEN
    SAY("In scenarios where an attack happends ");
    SAY("the Gantt Chart starts at the time of the attack");
    COORDINATE  $f: resend_fuel_through_pipeline
    DO
        ADD SAY("Fuel takes "$f.duration" days to travel through pipeline")
            PRECEDES $f;
    OD;
ELSE
    SAY("This scenario shows the timeline for the production and delivery of F24 jet fuel");
    COORDINATE  $f: send_fuel_through_pipeline
    DO
        ADD SAY("Fuel takes "$f.duration" days to travel through pipeline")
            PRECEDES $f;
    OD;
FI;

IF #repair_light_damage > 0 THEN
    SAY("Colonial_Pipeline takes light damage");
FI;
IF #repair_medium_damage > 0 THEN
    SAY("Colonial_Pipeline takes medium damage");
FI;
IF #repair_heavy_damage > 0 THEN
    SAY("Colonial_Pipeline takes heavy damage");
FI;

COORDINATE     $jba: stops_receiveing_F24_jet_fuel
    DO
        ADD SAY("On day " $jba.start" after the attack Joint Base Andrews stops receving fuel")
            PRECEDES $jba;
    OD;

COORDINATE     $jba: runs_out_of_F24_jet_fuel
    DO
        ADD SAY("On day " $jba.start" after the attack Joint Base Andrews runs out of jet fuel")
            PRECEDES $jba;
    OD;
IF #runs_out_of_F24_jet_fuel > 0 THEN
    COORDINATE
        $f: receive_F24_jet_fuel2,
        $g: runs_out_of_F24_jet_fuel
        DO
            ADD SAY($f.end-$g.start" days pass with Joint Base Andrews receving F24 jet fuel being unoperational")
                PRECEDES $f;
        OD;
FI;

IF #hacks_the_pressure_control_of_the_Colonial_Pipeline > 0 THEN
    COORDINATE
        $f: receive_F24_jet_fuel2,
        $g: stops_receiveing_F24_jet_fuel
        DO
            ADD SAY($f.end-$g.start" days pass without Joint Base Andrews receving F24 jet fuel")
                PRECEDES $f;
    OD;
FI;
```

Figure 25. MP Code for Jet Fuel Supply Chain Use Case. Source: Alden et al. (2020).

B. MP CODE FOR THE BARGE USE CASE

This MP software code is for the barge model. It was conceived by Nathan Alden, one of the student interns that developed the jet fuel supply chain model, and revised by Dr. Kristin Giammarco and the author.

```
/*
BargeAttackModel
created by Nathaniel Alden version 2.0 12-16-20, Baseline Supply Chain
modified by Margaret Palmieri, outcomes added
modified by Margaret Palmieri, added risk and probability
modified by Kristin Giammarco 01-14-21, regrouped attributes and added global report
modified by Mikhail Auguston 01-14-21, added calculations to global report
*/

SCHEMA Supply_Line

/* Roots for the Cyber Threat, DFSP Baltimore, and the Barge */

ROOT Cyber_Threat:  (   hacks_the_barge
                      (   tries_to_delay_the_barge    |
                          tries_to_sink_the_barge     )   |

                      no_impact
                                                          )
;


ROOT  DFSP_Baltimore:   send_barge_to_DFSP_Anacostia
;


ROOT Barge: leaves_for_DSFP_Anacostia
            (   navigation_systems_are_hacked
                (   barge_delayed arrives_at_DSFP_Anacostia |
                    barge_sunk                              )   |

                    arrives_at_DSFP_Anacostia
                                                              )
;

/* Establishes precedence and relationships */

COORDINATE  $x: send_barge_to_DFSP_Anacostia    FROM DFSP_Baltimore,
            $y: leaves_for_DSFP_Anacostia       FROM Barge
    DO ADD $x PRECEDES $y; OD;

COORDINATE  $x: hacks_the_barge                 FROM Cyber_Threat,
            $y: navigation_systems_are_hacked   FROM Barge
    DO ADD $x PRECEDES $y; OD;

COORDINATE  $x: tries_to_delay_the_barge        FROM Cyber_Threat,
            $y: barge_delayed                   FROM Barge
    DO ADD $x PRECEDES $y; OD;

COORDINATE  $x: tries_to_sink_the_barge         FROM Cyber_Threat,
            $y: barge_sunk                      FROM Barge
    DO ADD $x PRECEDES $y; OD;


/* Assigns attributes to calculate risk */

ATTRIBUTES{number likelihood, impact, sum_risk_scores,
               max_risk_score, max_risk_trace_unique_number;};

COORDINATE $no_attack: no_impact
    DO  $no_attack.likelihood:= 0.2;
        $no_attack.impact:= 1;
    OD;

COORDINATE $attack_to_delay: barge_delayed
    DO  $attack_to_delay.likelihood:= 0.8;
        $attack_to_delay.impact:= 5;
    OD;

COORDINATE $attack_to_destroy: barge_sunk
    DO  $attack_to_destroy.likelihood:= 0.2;
        $attack_to_destroy.impact:= 5;
    OD;


/* Calculates risk and creates SAY statements for
Likelihood, Impact Factor, and Risk Score. */

COORDINATE $y: ( no_impact | barge_delayed | barge_sunk )
    DO
           SAY("Likelihood: "$y.likelihood);
           SAY("Impact Factor: "$y.impact);
           SAY("Risk Score: "$y.likelihood*$y.impact);
```

```
/************************ GLOBAL Section *************************/

/*If the likelihood*impact for a given trace exceeds the current global maximum
risk factor value (initialized at zero), then make the max risk factor THIS
trace's risk factor and grab the trace id for the max risk trace.  */

        IF $y.likelihood*$y.impact > GLOBAL.max_risk_score THEN
            GLOBAL.max_risk_score:= $y.likelihood*$y.impact;
            GLOBAL.max_risk_trace_unique_number:= trace_id;
        FI;
        GLOBAL.sum_risk_scores +:= $y.likelihood*$y.impact;


/*MARK traces that have a risk factor greater than a certain value.*/

            IF $y.likelihood*$y.impact >= 4 THEN MARK; FI;
    OD;

/*Display a risk report before the results of each trace that includes:
total risk and highest risk, and sorts traces from highest to lowest risk. */

GRAPH risk_report{ };

GLOBAL
REPORT Global_Risk{TITLE("Risk Report for Scope " $$scope);};
WITHIN risk_report{ };

    SAY("Total risk over " #$$TRACE " traces: "
                                        GLOBAL.sum_risk_scores) => Global_Risk;
    SAY("Highest Risk: " GLOBAL.max_risk_score" at trace "
                                GLOBAL.max_risk_trace_unique_number) => Global_Risk;
    SAY("Sort by Marked to view traces with a risk factor >= 4.") => Global_Risk;

    SHOW Global_Risk;

/*****************************************************************/
```

Figure 26. MP Code for the Barge Use Case.

C. MP CODE FOR THE USE CASE WITH TWO CYBER THREATS

This MP software code is for the model with two cyber threats to the jet fuel supply chain. The author developed this model by combining and adapting code from the jet fuel supply chain model developed by the NSA interns and from the barge model developed by Nathan Alden and revised by Dr. Kristin Giammarco. Dr. Giammarco created the code in the global risk section and the author applied it to the use case with two threats.

```
/*
TwoThreatsModel
created by Nathaniel Alden version 2.0 12-16-20, Baseline Supply Chain
modified by Margaret Palmieri, outcomes added
modified by Margaret Palmieri, added risk and probability
modified by Kristin Giammarco 01-14-21, regrouped attributes and added global report
modified by Mikhail Auguston 01-14-21, added calculations to global report
modified by Kristin Giammarco 02-25-21, cleaned up comments
modified by Margaret Palmieri 07-29-21, added Pipeline use case, updated global report for two scenarios
modified by Kristin Giammarco 08-01-21, revised global report model for two scenarios
modified by Margaret Palmieri 08-03-21, updated attributes and model notes
*/

SCHEMA Supply_Line


;
ROOT Cyber_Threat1:
    (
        hacks_the_pressure_control_of_the_Colonial_Pipeline |
    do_nothing
    )
;

ROOT Colonial_Pipeline:
    receive_jet_fuel
    send_fuel_through_pipeline
    [
        pipeline_bursts
        fuel_is_halted
        (
            repair_light_damage |
            repair_medium_damage |
            repair_heavy_damage
                )
        resend_fuel_through_pipeline
    ]
    arrives_at_end_point
;

/**/
COORDINATE    $x: hacks_the_pressure_control_of_the_Colonial_Pipeline     FROM Cyber_Threat1,
              $y: pipeline_bursts FROM Colonial_Pipeline
    DO ADD $x PRECEDES $y; OD;
/**/

ROOT  DFSP_Baltimore:
    receive_jet_fuel
    tranform_jet_fuel_into_F24_jet_fuel
    put_into_storage_tanks
    load_onto_barge
    send_barge_to_DFSP_Anacostia
;
/**/
COORDINATE    $x: arrives_at_end_point     FROM Colonial_Pipeline,
              $y: receive_jet_fuel FROM DFSP_Baltimore
    DO ADD $x PRECEDES $y; OD;
/**/
/**/

ROOT Barge: leaves_for_DSFP_Anacostia
            (   navigation_systems_are_hacked
                (   barge_delayed arrives_at_DSFP_Anacostia |
                    barge_sunk                              )   |

                    arrives_at_DSFP_Anacostia
                                                              )
;

ROOT Cyber_Threat2: (  hacks_the_barge
                       (   tries_to_delay_the_barge    |
                           tries_to_sink_the_barge     )   |

                     no_impact
                                                      )
;
COORDINATE  $x: send_barge_to_DFSP_Anacostia    FROM DFSP_Baltimore,
            $y: leaves_for_DSFP_Anacostia       FROM Barge
    DO ADD $x PRECEDES $y; OD;

COORDINATE  $x: hacks_the_barge                 FROM Cyber_Threat2,
            $y: navigation_systems_are_hacked   FROM Barge
    DO ADD $x PRECEDES $y; OD;

COORDINATE  $x: tries_to_delay_the_barge        FROM Cyber_Threat2,
            $y: barge_delayed                   FROM Barge
    DO ADD $x PRECEDES $y; OD;

COORDINATE  $x: tries_to_sink_the_barge         FROM Cyber_Threat2,
            $y: barge_sunk                      FROM Barge
    DO ADD $x PRECEDES $y; OD;
```

```
/**/
/*Remaining nodes to complete the supply chain.
Activate this line to see entire supply chain.*/
/*
ROOT  DFSP_Anacostia:
    receive_F24_jet_fuel
    check_quality_and_amount
    send_to_Joint_Base_Andrews
    ;

COORDINATE    $x: arrives_at_DSFP_Anacostia         FROM Barge,
              $y: receive_F24_jet_fuel              FROM DFSP_Anacostia
    DO ADD $x PRECEDES $y; OD;

ROOT Joint_Base_Andrews:
    receive_F24_jet_fuel
    use_F24_jet_fuel
;

COORDINATE    $x: send_to_Joint_Base_Andrews     FROM DFSP_Anacostia,
              $y: receive_F24_jet_fuel FROM Joint_Base_Andrews
    DO ADD $x PRECEDES $y; OD;

/**/

/* Attribute Assignments:
Definitions of attributes are combined into one ATTRIBUTES
statement. Attributes include likelihood and impact to calculate risk,
and attributes used in global risk report.*/


/*Attribute "trace_risk_score" stores the sum of the PIPELINE + BARGE RISKS */
ATTRIBUTES{number likelihood, impact, trace_risk_score, sum_risk_score,
                max_risk_score, max_risk_trace_unique_number;};

/* Assigns attributes for the Colonial Pipeline use case */

COORDINATE $no_pipe_attack: do_nothing
    DO  $no_pipe_attack.likelihood:= 0.2;
        $no_pipe_attack.impact:= 1;
    OD;

COORDINATE $attack_bursts_pipeline: repair_light_damage
    DO  $attack_bursts_pipeline.likelihood:= 0.8;
        $attack_bursts_pipeline.impact:= 7;
    OD;

COORDINATE $attack_bursts_pipeline: repair_medium_damage
    DO  $attack_bursts_pipeline.likelihood:= 0.8;
        $attack_bursts_pipeline.impact:= 9;
    OD;

COORDINATE $repair_complete_6days: repair_heavy_damage
    DO  $repair_complete_6days.likelihood:= 0.6;
        $repair_complete_6days.impact:= 9;
    OD;

/* Assigns attributes for the Barge use case */

COORDINATE $no_barge_attack: no_impact
    DO  $no_barge_attack.likelihood:= 0.2;
        $no_barge_attack.impact:= 1;
    OD;

COORDINATE $attack_to_delay: barge_delayed
    DO  $attack_to_delay.likelihood:= 0.8;
        $attack_to_delay.impact:= 5;
    OD;

COORDINATE $attack_to_destroy: barge_sunk
    DO  $attack_to_destroy.likelihood:= 0.2;
        $attack_to_destroy.impact:= 5;
    OD;

/**********Global Risk Section**********/


/*Calculate Risk Across Scenarios*/

/*OUTER COORDINATE GETS PIPELINE CONTRIBUTION TO RISK*/
COORDINATE $y: ( do_nothing | repair_light_damage | repair_medium_damage | repair_heavy_damage)

    /*INNER COORDINATE GETS BARGE CONTRIBUTION TO RISK*/
    DO COORDINATE $z: ( no_impact | barge_delayed | barge_sunk )
        DO

        /*GET THE TOTAL RISK SCORE FOR EACH TRACE (PIPELINE + BARGE)*/
        trace_risk_score+:= ($y.likelihood*$y.impact) + ($z.likelihood*$z.impact);

        /*Display risk attributes for the scenario*/
        SAY("Pipeline Likelihood: "$y.likelihood", Pipeline Impact: "$y.impact", Pipeline Risk Score: "$y.likelihood*$y.impact);
        SAY("Barge Likelihood: "$z.likelihood", Barge Impact: "$z.impact", Barge Risk Score: "$z.likelihood*$z.impact);


/*Sort results*/

        /*If the TRACE_RISK_SCORE for a given trace exceeds the current global maximum
        risk factor value (initialized at zero), then make the max risk factor THIS
        trace's risk factor and grab the trace id for the max risk trace.  */

        IF  trace_risk_score > GLOBAL.max_risk_score THEN
            GLOBAL.max_risk_score:= trace_risk_score;
            GLOBAL.max_risk_trace_unique_number:= trace_id;
        FI;

            /*MARK traces that have a risk factor greater than a certain value*/

            IF trace_risk_score >= 9 THEN MARK; FI;
        OD;
    OD;
```

```
/*Calculate Total Risk*/

/*Sum up risk scores across all traces*/
GLOBAL.sum_risk_score +:= trace_risk_score;

    /*ADD THE TOTAL RISK FOR EACH TRACE (PIPELINE + BARGE)*/
    SAY("Total Trace Risk: "trace_risk_score);


/*Create and Display Global Risk Report*/

GLOBAL
REPORT Global_Risk{TITLE("Risk Report for Scope " $$scope);};

/*Include these SAY statements in the Global_Risk REPORT. */
SAY("Total risk over " #$$TRACE " traces (sum of trace risk scores): "
                                    GLOBAL.sum_risk_score) => Global_Risk;
SAY("Highest Risk: " GLOBAL.max_risk_score" (trace "
                            GLOBAL.max_risk_trace_unique_number")") => Global_Risk;
SAY("Average Risk: " GLOBAL.sum_risk_score/#$$TRACE)
   => Global_Risk;
SAY("Sort by Marked to view traces with above average risk >=9.") => Global_Risk;

SHOW Global_Risk;

/************************************/
```

Figure 27. MP Code for Model with Two Cyber Threats.

D. MP CODE FOR MORE THAN TWO CYBER THREATS

This MP software code is for models with more than two cyber threats or iterative processes. It was developed by Dr. Kristin Giammarco while validating the model with two cyber threats in Section C. The main changes from the Section C model occur in the global section of the model.

```
/*
Two-Cyber-Threats-Model
created by Nathaniel Alden version 2.0 12-16-20, Baseline Supply Chain
modified by Margaret Palmieri, outcomes added
modified by Margaret Palmieri, added risk and probability
modified by Kristin Giammarco 01-14-21, regrouped attributes and added global report
modified by Mikhail Auguston 01-14-21, added calculations to global report
modified by Kristin Giammarco 02-25-21, cleaned up comments
modified by Margaret Palmieri 07-29-21, added Pipeline use case, updated global report for two scenarios
modified by Kristin Giammarco 08-01-21, revised global report model for two scenarios
modified by Margaret Palmieri 08-03-21, updated attributes and model notes
*/

SCHEMA Supply_Line


;
ROOT Cyber_Threat1:
    (
        hacks_the_pressure_control_of_the_Colonial_Pipeline |
    do_nothing
    )
;

ROOT Colonial_Pipeline:
    receive_jet_fuel
    send_fuel_through_pipeline
    [
        pipeline_bursts
        fuel_is_halted
        (
            repair_light_damage |
            repair_medium_damage |
            repair_heavy_damage
                )
        resend_fuel_through_pipeline
    ]
    arrives_at_end_point
;
```

```
/**/
COORDINATE    $x: hacks_the_pressure_control_of_the_Colonial_Pipeline     FROM Cyber_Threat1,
           $y: pipeline_bursts FROM Colonial_Pipeline
    DO ADD $x PRECEDES $y; OD;
/**/

ROOT  DFSP_Baltimore:
    receive_jet_fuel
    tranform_jet_fuel_into_F24_jet_fuel
    put_into_storage_tanks
    load_onto_barge
    send_barge_to_DFSP_Anacostia
;
/**/
COORDINATE    $x: arrives_at_end_point     FROM Colonial_Pipeline,
           $y: receive_jet_fuel FROM DFSP_Baltimore
    DO ADD $x PRECEDES $y; OD;
/**/

ROOT Barge: leaves_for_DSFP_Anacostia
            (   navigation_systems_are_hacked
                (   barge_delayed arrives_at_DSFP_Anacostia |
                    barge_sunk                              )   |

                    arrives_at_DSFP_Anacostia
                                                            )
;

ROOT Cyber_Threat2: (   hacks_the_barge
                        (   tries_to_delay_the_barge    |
                            tries_to_sink_the_barge     )   |

                        no_impact
                                                        )
;
COORDINATE  $x: send_barge_to_DFSP_Anacostia    FROM DFSP_Baltimore,
            $y: leaves_for_DSFP_Anacostia       FROM Barge
    DO ADD $x PRECEDES $y; OD;

COORDINATE  $x: hacks_the_barge                 FROM Cyber_Threat2,
            $y: navigation_systems_are_hacked   FROM Barge
    DO ADD $x PRECEDES $y; OD;

COORDINATE  $x: tries_to_delay_the_barge        FROM Cyber_Threat2,
            $y: barge_delayed                   FROM Barge
    DO ADD $x PRECEDES $y; OD;

COORDINATE  $x: tries_to_sink_the_barge         FROM Cyber_Threat2,
            $y: barge_sunk                      FROM Barge
    DO ADD $x PRECEDES $y; OD;

/**/
/*Remaining nodes to complete the supply chain.
Activate this line to see entire supply chain.*/
/*
ROOT  DFSP_Anacostia:
    receive_F24_jet_fuel
    check_quality_and_amount
    send_to_Joint_Base_Andrews
    ;

COORDINATE    $x: arrives_at_DSFP_Anacostia         FROM Barge,
              $y: receive_F24_jet_fuel              FROM DFSP_Anacostia
    DO ADD $x PRECEDES $y; OD;

ROOT Joint_Base_Andrews:
    receive_F24_jet_fuel
    use_F24_jet_fuel
;

COORDINATE    $x: send_to_Joint_Base_Andrews     FROM DFSP_Anacostia,
              $y: receive_F24_jet_fuel FROM Joint_Base_Andrews
    DO ADD $x PRECEDES $y; OD;

/**/

/* Attribute Assignments:
Definitions of attributes are combined into one ATTRIBUTES
statement. Attributes include likelihood and impact to calculate risk,
and attributes used in global risk report.*/
```

```
/*Attribute "trace_risk_score" stores the sum of the PIPELINE = BARGE RISKS */
ATTRIBUTES{number likelihood, impact, trace_risk_score, sum_risk_score,
                max_risk_score, max_risk_trace_unique_number;};

/* Assigns attributes for the Colonial Pipeline use case */

COORDINATE $no_pipe_attack: do_nothing
    DO  $no_pipe_attack.likelihood:= 0.2;
        $no_pipe_attack.impact:= 1;
    OD;

COORDINATE $attack_bursts_pipeline: repair_light_damage
    DO  $attack_bursts_pipeline.likelihood:= 0.8;
        $attack_bursts_pipeline.impact:= 7;
    OD;

COORDINATE $attack_bursts_pipeline: repair_medium_damage
    DO  $attack_bursts_pipeline.likelihood:= 0.8;
        $attack_bursts_pipeline.impact:= 9;
    OD;

COORDINATE $repair_complete_6days: repair_heavy_damage
    DO  $repair_complete_6days.likelihood:= 0.6;
        $repair_complete_6days.impact:= 9;
    OD;

/* Assigns attributes for the Barge use case */

COORDINATE $no_barge_attack: no_impact
    DO  $no_barge_attack.likelihood:= 0.2;
        $no_barge_attack.impact:= 1;
    OD;

COORDINATE $attack_to_delay: barge_delayed
    DO  $attack_to_delay.likelihood:= 0.8;
        $attack_to_delay.impact:= 5;
    OD;

COORDINATE $attack_to_destroy: barge_sunk
    DO  $attack_to_destroy.likelihood:= 0.2;
        $attack_to_destroy.impact:= 5;
    OD;

/**********Global Risk Section**********/

/*Calculate Risk Across Scenarios*/

/* Trace Risk Table and Summary */

TABLE event_risks{
    TITLE ("Event Risks");
    TABS    string Event,
            string Likelihood,
            string Impact,
            string Risk_Score;
};
    CLEAR event_risks;

COORDINATE $e: $$EVENT
    DO  trace_risk_score+:= ($e.likelihood*$e.impact);
        IF ($e.likelihood*$e.impact) > 0 THEN
                event_risks <|
                    Event: SAY($e),
                    Likelihood: SAY($e.likelihood),
                    Impact: SAY($e.impact),
                    Risk_Score: SAY($e.likelihood*$e.impact);
        FI;
```

```
/*Sort results*/

        /*If the TRACE RISK SCORE for a given trace exceeds the current global maximum
        risk factor value (initialized at zero), then make the max risk factor THIS
        trace's risk factor and grab the trace id for the max risk trace.  */
        IF  trace_risk_score > GLOBAL.max_risk_score THEN
            GLOBAL.max_risk_score:= trace_risk_score;
            GLOBAL.max_risk_trace_unique_number:= trace_id;
        FI;

            /*MARK traces that have a risk factor greater than a certain value*/

            IF trace_risk_score >= 9 THEN MARK; FI;
    OD;

IF trace_risk_score > 0 THEN    SHOW event_risks;
                                SAY("Total Trace Risk: "trace_risk_score);
FI;


/*Calculate Total Risk*/

/*Sum up risk scores across all traces*/
GLOBAL.sum_risk_score +:= trace_risk_score;


/*Create and Display Global Risk Report*/

GLOBAL
REPORT Global_Risk{TITLE("Risk Report for Scope " $$scope);};

/*Include these SAY statements in the Global_Risk REPORT. */
SAY("Total risk over " #$$TRACE " traces (sum of trace risk scores): "
                                    GLOBAL.sum_risk_score) => Global_Risk;
SAY("Highest Risk: " GLOBAL.max_risk_score" (trace "
                                GLOBAL.max_risk_trace_unique_number")") => Global_Risk;
SAY("Average Risk: " GLOBAL.sum_risk_score/#$$TRACE)
    => Global_Risk;
SAY("Sort by Marked to view traces with above average risk >=9.") => Global_Risk;

SHOW Global_Risk;

/*************************************/
```

Figure 28. MP Code for Model with More than Two Cyber Threats.

LIST OF REFERENCES

Alden, Nathan, Jessica Dahl, Oybek Kamalov, Troy Smith, Rachel Talkington, Rachel Thompson, Noah Wells, and David Zhao. 2020. "Enterprise Risk Management." Unpublished presentation, July 25, 2020. https://nps.app.box.com/s/ber4qe65vzbk2lpip4nwvqm9euqxk5u1.

Auguston, Mikhail. 2009. "Monterey Phoenix, or How to Make Software Architecture Executable." OOPSLA09/Onward conference, OOPSLA Companion, October 2009, pp.1031-1038. Accessed June 30, 2021. http://hdl.handle.net/10945/36348.

Auguston, Michael. 2020. *Monterey Phoenix, System and Software Behavior Modeling Language (version 4.0).* Monterey, CA: Naval Postgraduate School, March 2020. Accessed June 28, 2021. https://wiki.nps.edu/download/attachments/604667916/MP2-syntax-v4.pdf

Burke, David A., and Edward Morgan. 2018. "NAVAIR Cyber Risk Assessment." Presentation to the Project Management Institute Southern Maryland Chapter. June 19, 2018. https://pmisomd.org/events/presentations/609-20180619-cwd-cra-briefing/file.

Cape Charles Municipal Government. N.d. "Distances Between United States Ports." Accessed July 30, 2021. https://capecharles.municipalcms.com/files/documents/document1463023404091913.pdf.

Consultancy.org. 2018. "Global Risk Consulting Market Nears $70 Billion, Top 30 Consultancy Firms." December 13, 2018. https://www.consultancy.org/news/101/global-risk-consulting-market-nears-70-billion-top-30-consultancy-firms.

Dickinson, Gerry. 2001. "Enterprise Risk Management: Its Origins and Conceptual Foundation." *Geneva Papers on Risk and Insurance–Issues and Practice* 26 (3):360–366. DOI:10.1111/1468-0440.00121.

Gallistel, C. Randy. 2015. "Bayes for Beginners: Probability and Likelihood." *Observer* 28 (7) (September). https://www.psychologicalscience.org/observer/bayes-for-beginners-probability-and-likelihood.

Ghadge, Abhijeet, Maximilian Weiß, Nigel D Caldwell, and Richard Wilding. 2019. "Managing Cyber Risk in Supply Chains: A Review and Research Agenda." *Supply Chain Management* 25 (2): 223–40. https://doi.org/10.1108/SCM-10-2018-0357.

Giammarco, Kristin, Mikhail Auguston, W. Clifton Baldwin, Ji'on Crump, and Monica Farah-Stapleton. 2014. "Controlling Design Complexity with the Monterey Phoenix Approach." *Procedia Computer Science*, 36 (2014): 204–209. https://doi.org/10.1016/j.procs.2014.09.080.

Giammarco, Kristin, and Mikhail Auguston. 2019. "Monterey Phoenix—Behavior Modeling Approach for the Early Verification and Validation of System of Systems Emergent Behaviors." In *Engineering Emergence*, 1st ed., 1: 357–88. Routledge. https://doi.org/10.1201/9781138046412-18.

Goldsby, Thomas, Deepak Iyengar, and Shashank Rao. 2014. *Definitive Guide to Transportation, The Principles, Strategies, and Decisions for the Effective Flow of Goods and Services*. Hoboken, NJ: Pearson FT Press.

Heaton, Tyrell. 2010. "113th receives newer, more capable F-16s." 113th Wing. Last modified April 19, 2010. https://www.113wg.ang.af.mil/News/Article-Display/Article/448015/113th-receives-newer-more-capable-f-16s/.

Ho, William, Tian Zheng, Hakan Yildiz, and Srinivas Talluri. 2015. "Supply Chain Risk Management: A Literature Review." International Journal of Production Research 53 (16): 5031–69. https://doi.org/10.1080/00207543.2015.1030467.

Inman, Ronald. "Refinery to Flight." 2017. Defense Logistics Agency News website, November 1, 2017. Accessed May 25, 2017. https://www.dla.mil/AboutDLA/News/NewsArticleView/Article/1370566/refinery-to-flight.

International Association of Transatlantic Airlines (IATA). 2021. "Jet Fuel Price Monitor." Last modified July 23, 2021. https://www.iata.org/en/publications/economics/fuel-monitor/.

Kodable. 2019. "How to Teach Kids About Loops: Crash Course for Teachers." YouTube video, May 21, 2019. 2:06. https://www.youtube.com/watch?v=uVVSopz56ek&t=3s.

Merlin Petroleum. N.d. "Barge Rates." Accessed July 29, 2021. http://www.merlinpetroleum.com/bargerates.htm.

Moebius, Richard C. 2018. "Methods and Tool for Risk Analysis Based on Behavior Models Utilizing Monterey Phoenix." Master's thesis, Naval Postgraduate School.

National Aeronautic Space Agency. 2011. *NASA Risk Management Handbook*. Washington, DC. https://ntrs.nasa.gov/citations/20120000033.

Naval Postgraduate School (NPS). 2021. "Monterey Phoenix Home." Last modified February 24, 2021. https://wiki.nps.edu/display/MP.

Office of the Deputy Assistant Secretary of Defense for Systems Engineering. 2017. *Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs*. Washington, D.C., https://acqnotes.com/wp-content/uploads/2017/07/DOD-Risk-Issue-and-Opportunity-Management-Guide-Jan-2017.pdf.

Project Management Institute. 2013. *A Guide to the Project Management Body of Knowledge.* Fifth Edition. Newtown Square, PA.

Quartuccio, John J. and Kristin M. Giammarco. 2019. "A Model-Based Approach to Investigate Emergent Behaviors in Systems of Systems." In *Engineering Emergence*, 1st ed., 1:389–458. Routledge. https://doi.org/10.1201/9781138046412-19.

Rumsfeld, Donald H. 2002. "DOD News Briefing—Secretary Rumsfeld and Gen. Myers." U.S. Department of Defense. February 12, 2002. https://archive.ph/20180320091111/http://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636.

Sigalos, MacKenzie. 2021. "Colonial Pipeline Cyber-Attack is No Cause for Panic—Here's Why." CNBC. May 12, 2021. https://www.cnbc.com/2021/05/14/colonial-pipeline-hack-doesnt-mean-more-ransomware-attacks-critical-infrastructure.html.

Smith, Preston G., and Guy M. Merritt. 2002. *Proactive Risk Management: Controlling Uncertainty in Product Development*. New York, NY: Productivity Press.

Smith, Preston G., and Guy M. Merritt. 2004. "Techniques for Managing Project Risk." In *Field Guide to Project Management. 2nd edition*, edited by David I Cleland, 202–218. Hoboken, NJ: J. Wiley. https://doi.org/10.1002/9780470172346.

Turton, William, and Kartikay Mehrotra. 2021. "Hackers Breached Colonial Pipeline Using Compromised Password." Bloomberg Online, June 4, 2021. Accessed July 2, 2021. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.

U.S. Air Force. N.d.. "113th Wing." Accessed July 29, 2021. https://www.113wg.ang.af.mil/aboutus/.

U.S. Air Force. 2015. "F-16 Fighting Falcon." Last modified September 23, 2015. https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104505/f-16-fighting-falcon/.

Weeks Marine. 2021. "Tugboats." Accessed July 30, 2021. https://www.weeksmarine.com/equipment-division/tugboats.

Wolke, Thomas. 2017. *Risk Management*. München: De Gruyter Oldenbourg. https://doi.org/10.1515/9783110440539.

Zhang, Xiao, and Jie Han. 2011. “Analysis on the Importance of Nodes in Supply Chain Network.” 2011 International Conference on Business Computing and Global Informatization, 387–388. https://doi.org/10.1109/BCGIn.2011.103.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California